Data Protection in Humanitarian Action

Responding to Crises in a Data-Driven World

Edited by
Ana Beduschi, Massimo Marelli, and Aaron Martin

ROUTLEDGE
GPA Global Privacy Assembly
ICRC
UNHCR The UN Refugee Agency

"In our changing world, knowledge production is key to understanding where we stand in the digital age. This timely publication makes a valuable contribution by placing data protection at the center, as an enabler of rights and a vital tool to strengthen humanitarian action."

— **Beatriz de Anchorena**, *Chair of the Committee of Convention 108 and Head of the AAIP, the Data Protection Authority in Argentina.*

"A timely and thoughtful reflection on a decade of progress in data protection across the humanitarian sector, and a vital guide as we navigate our increasingly data-driven world."

— **Carmen Casado**, *DPO and Director of the Global Privacy Office, UN World Food Programme*

"Data protection has become a crucial topic in the humanitarian space. This new book examining the interface between data protection regulatory frameworks and humanitarian action will be mandatory reading for anyone working in either field."

— **Christopher Kuner (Dr),** *University of Copenhagen and Wilson Sonsini Goodrich & Rosati, Brussels.*

"This timely publication captures a decade of critical reflection on data protection as a cornerstone of principled and effective humanitarian action. Bridging theory and practice, it reaffirms our collective commitment to dignity, trust, and accountability in a digital age – and equips us to face emerging challenges with integrity."

— **Lucie Laplante**, *Under Secretary General for Legal, Governance and Accountability, ad interim, IFRC.*

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

DATA PROTECTION IN HUMANITARIAN ACTION

This book is the product of a collaboration between the data protection offices of the ICRC and UNHCR, alongside the Global Privacy Assembly, to reflect on a decade of progress in data protection in humanitarian contexts. Through practitioner perspectives, empirical research, and conceptual reflections, it examines how data protection underpins trust, accountability, and respect for affected populations, serving as a crucial enabler for ethical and effective humanitarian action in the digital age.

The volume explores critical topics including digital transformation, operational complexities such as those linked to data breaches and data sharing, regulatory developments and international cooperation, legal frameworks and capacity-building. At the same time, it looks ahead, addressing the challenges and opportunities posed by emerging technologies and considering how the humanitarian sector may anticipate and prepare for them.

This book is intended for policymakers, practitioners, authorities, academics, and other experts working in data protection, international organisations, and humanitarian action and adjacent fields. It offers a compass to help navigate complex operational and legal challenges in an increasingly digital and data-driven landscape. By positioning data protection as a foundational element of humanitarian action, the book provides timely, forward-looking insights into the sector's preparedness for technological and regulatory change, with the aim of helping those most in need.

Ana Beduschi is a Full Professor of Law with a Personal Chair at the University of Exeter. Her research and teaching focus on international human rights law, technology (including big data and artificial intelligence), data protection, and international migration and refugee law.

Massimo Marelli is the Head of the Data Protection Office at the International Committee of the Red Cross. He is also a member of the Advisory Board and a Fellow at the European Centre on Privacy and Cybersecurity at the University of Maastricht, where he co-leads the Humanitarian Action Programme.

Aaron Martin is an Assistant Professor of Media Studies and Data Science at the University of Virginia, United States. His research interests include data governance in development and humanitarian contexts, critical infrastructure protection, surveillance, and biometrics.

DATA PROTECTION IN HUMANITARIAN ACTION

Responding to Crises in a Data-Driven World

Edited by Ana Beduschi, Massimo Marelli, and Aaron Martin

Managing Editors: Maria Haas, Silvia Pelucchi, and Jie Yang

This volume is a collaborative effort initiated by the Data Protection Office at the ICRC, the Data Protection Office at the UNHCR, and the GPA Working Group Aid, to mark the 10th year of the ICRC and UNHCR data protection frameworks, and the GPA Resolution on Privacy and International Humanitarian Action. The opinions and views expressed in this volume are the contributors' own and do not necessarily represent those of these organizations.

Maastricht University
ECPC
European Centre on Privacy & Cybersecurity

This volume is published in cooperation with the Humanitarian Action Programme at the European Centre on Privacy and Cybersecurity at Maastricht University.

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Designed cover image: by twks for the 2019 Digital Dilemmas project for the ICRC, on the occasion of the 33rd International Conference of the Red Cross Red Crescent Movement.

First published 2026
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Beduschi, Ana editor | Marelli, Massimo, 1979- editor | Martin, Aaron (Writer on Data Protection) editor
Title: Data protection in humanitarian action : responding to crises in a data-driven world / edited by Ana Beduschi, Massimo Marelli, and Aaron Martin ; managing editors, Maria Haas, Silvia Pelucchi, and Jie Yang.
Description: Abingdon, Oxon [UK] ; New York, NY : Routledge, 2026. | Includes bibliographical references and index.
Identifiers: LCCN 2025031732 | ISBN 9781041094074 hardback | ISBN 9781041094586 paperback | ISBN 9781003650164 ebook
Subjects: LCSH: Office of the United Nations High Commissioner for Refugees | International Committee of the Red Cross. Advisory Service on International Humanitarian Law | Humanitarian law | Data protection--Law and legislation | Privacy, Right of | Information technology--Law and legislation | Humanitarian intervention
Classification: LCC KZ6471 .D39 2026 | DDC 341.6/7--dc23/eng/20250718
LC record available at https://lccn.loc.gov/2025031732

ISBN: 978-1-041-09407-4 (hbk)
ISBN: 978-1-041-09458-6 (pbk)
ISBN: 978-1-003-65016-4 (ebk)

DOI: 10.4324/9781003650164

Typeset in Galliard
by Deanta Global Publishing Services, Chennai, India

CONTENTS

LIST OF ABBREVIATIONS

AADMER	ASEAN Agreement on Disaster Management and Emergency Response
AFAPDP	*Association Francophone des Autorités de Protection des Données Personnelles*
AI	Artificial Intelligence
ALNAP	Active Learning Network for Accountability and Performance
APDP	Monegasque Personal Data Protection Authority
APEC	Asia-Pacific Economic Cooperation
APPA	Asia Pacific Privacy Authorities
ASEAN	Association of Southeast Asian Nations
CCD	Collaborative Cash Delivery Network
CETS	Council of Europe Treaty Series
CFIP	Concern for Information Privacy
CNIL	*Commission Nationale de l'Informatique et des Libertés*
CoP	Community of Practice
CTA	Central Tracing Agency
CVA	Cash and Voucher Assistance
CWG	Ukraine Cash Working Group
DFFT	Data Free Flow with Trust
DPA	Data Protection Authority
DPGA	Digital Public Goods Alliance
DPI	Digital Public Infrastructure
DPIA	Data Protection Impact Assessment

DPL	Data Protection Legislation
DPOHA	Data Protection Officer in Humanitarian Action
DPORF	Data Protection and Other Rights and Freedoms Working Group
DSA	Data Sharing Agreement
EASO	European Asylum Support Office
EC	European Commission
ECHR	European Convention on Human Rights
ECPC	European Centre on Privacy and Cybersecurity
EDFI	Association of European Development Finance Institutions
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eKYC	electronic Know Your Customer
ELM	Elaboration Likelihood Model
EPFL	*École Polytechnique Fédérale de Lausanne*
ETC	Emergency Telecommunications Cluster
ETH	Federal Institute of Technology Zurich
EEA	European Economic Area
EU	European Union
EUAA	European Union Agency for Asylum
FDPIC	Swiss Federal Data Protection and Information Commissioner
FLN	Family Links Network
FRTA	Family Reunion Travel Assistance
GDPP	General Policy on Personal Data Protection and Privacy
GDPR	General Data Protection Regulation
GHDI	Good Humanitarian Donorship Initiative
GPA	Global Privacy Assembly
GSMA	Global System for Mobile Communications Association
HDTI	Humanitarian Data and Trust Initiative
HESPER	Humanitarian Emergency Settings Perceived Needs Scale
HPG	Humanitarian Policy Group
IASC	Inter-Agency Standing Committee
ICDPPC	International Conference of Data Protection and Privacy Commissioners
ICMP	International Commission on Missing Persons
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICVA	International Council of Voluntary Agencies
ID4D	Identification for Development
IEWG	International Enforcement Cooperation Working Group
IFRC	International Federation of Red Cross and Red Crescent Societies
IO	International Organisation

IOM	International Organization for Migration
IRC	International Rescue Committee
ITU	International Telecommunication Union
INTERPOL	International Criminal Police Organization
IUIPC	Internet Users' Information Privacy Concerns
KII	Key Informant Interview
LEO	Low Earth Orbit
MCTD	Minderoo Centre for Technology & Democracy
MFEA	Ministry of Foreign and European Affairs Of Luxembourg
MIS	Management Information System
MNO	Mobile Network Operator
Movement	International Red Cross and Red Crescent Movement
MPCA	Multi-Purpose Cash Assistance
MSF	Médecins Sans Frontières
NADPA	Network of African Data Protection Authorities
NCHS	Norwegian Centre for Humanitarian Studies
NGO	Non-governmental organisation
NIIHA	Neutral, Impartial, Independent Humanitarian Action
OAS	Organization of American States
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
ODPC	Kenyan Office of the Data Protection Commissioner
OECD	Organisation for Economic Co-operation and Development
OECD-DAC	Organisation for Economic Co-operation and Development's Development Assistance Committee
PBL	Problem-Based Learning
PIPEDA	Personal Information Protection and Electronic Documents Act
RFL	Restoring Family Links
RIPD	Ibero-American Data Protection Network
SAR	Synthetic Aperture Radar
SDG	Sustainable Development Goals
SLRC	Secure Livelihoods Research Consortium
SMM	Social Media Monitoring
TIN	Tax Identification Number
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations International Children's Emergency Fund
UNLC	United Nations Legal Counsel
UNOOSA	United Nations Office for Outer Space Affairs
UNOSAT	United Nations Satellite Centre
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
UPI	Unified Payment Interface

VPN	Virtual Private Network
WG AID	Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management
WHO	World Health Organization
WFP	World Food Programme

LIST OF CONTRIBUTORS

Ana Beduschi is a Full Professor of Law with a Personal Chair at the University of Exeter. Her research and teaching focus on international human rights law, technology (including big data and artificial intelligence), data protection, and international migration and refugee law.

Romain Bircher is the Leader of the Digital Platform Challenge Team at the International Committee of the Red Cross (ICRC), Switzerland. He has worked with the ICRC for over 30 years, particularly in conflicts and situations of violence, and on humanitarian and digital initiatives such as Restoring Family Links and RedSafe.

Dogu Han Buyukyagcioglu is a member of the Data Protection Office of the United Nations High Commissioner for Refugees (UNHCR), where he is the lead for development of policy and guidance material. He also advises the headquarters and field operations on the implementation of UNHCR's data protection and privacy standards.

Stuart Campo is the Senior Advisor on Data Impact, Strategy and Partnerships at the International Organization for Migration. He has over seventeen years of experience in the humanitarian sector, with a focus on the safe, ethical, and effective use of data and digital technology in complex environments.

Gilles Cerutti is the Head of the Humanitarian Diplomacy Section at the Swiss Federal Department of Foreign Affairs' Peace and Human Rights Division. His work focuses on the protection of civilians in conflict, including from digital threats, through diplomacy, multilateral engagement, and policy development.

Timothy Charlton is a Postdoctoral Research Associate at the Minderoo Centre for Technology and Democracy, University of Cambridge, and a Junior Research Fellow of Wolfson College, Cambridge. His research explores the digital infrastructure of principled humanitarian action and how affected communities perceive the handling of their personal data.

Florence Dubosc is a legal officer at the Monegasque Data Protection Authority, where she heads the Compliance and International Division. Since 2020 she is co-chairing the Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management of the Global Privacy Assembly.

Michèle Dubrocard is a Legal Officer at European Data Protection Supervisor. A judge in her home country, she has also worked as a national expert seconded to the Secretariat of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. She has recently been appointed as Distinguished External Jurist of the Justice Committee of the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA).

David Erdos is a WYNG Fellow in Law at Trinity Hall and Professor of Law and the Open Society, and Co-Director of the Centre for Intellectual Property and Information Law, Faculty of Law, University of Cambridge. His current research focuses on information law and also national and international public law and its history.

Larissa Fast is Professor of Humanitarian and Conflict Studies at the Humanitarian and Conflict Response Institute, University of Manchester. She researches and writes about data and technology in the humanitarian sector, and about violence against and the protection of civilians, particularly aid workers and healthcare workers.

Julia Feigen is a Doctoral Fellow at the Minderoo Centre for Technology and Democracy, at the University of Cambridge. As a PhD Candidate in Geography, her work focuses on humanitarian action, international armed conflict, and digital technologies.

Natalie Klein-Kelly holds degrees in history and international development from Mainz (Germany), Cambridge (UK), and Lucerne (Switzerland), and has worked for the International Committee of the Red Cross in the field of protection, both globally and in Geneva, for over two decades.

Emily Knox is the Head of Restoring Family Links for the British Red Cross, overseeing the International Family Tracing service and Family Reunion services.

Christina Vasala Kokkinaki is a Senior Legal Officer with the Legal Affairs Unit of the International Telecommunication Union (ITU), where she works on a range of legal issues, including privileges and immunities, and currently leads the taskforce for the development and implementation of ITU's Data Protection Policy.

Sophie Kwasny is responsible for Education, Training and Cooperation in the Youth Department of the Council of Europe. She used to be responsible for standard-setting and policy on data protection and privacy from 2011 to 2021 and has been working for the Council of Europe for over 25 years.

Catherine Lennman is the delegate for international affairs and Francophonie at the Swiss Federal Data Protection and Information Commissioner. Since 2020, she is chairing the Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management of the Global Privacy Assembly.

Charlotte Lindsey Curtet is currently an independent consultant, Research Fellow (remote) with the Berkeley Human Rights Center, and co-CEO of Neutrality Sàrl, a Swiss tech startup.

Massimo Marelli is the Head of the Data Protection Office at the International Committee of the Red Cross. He is also a member of the Advisory Board and a Fellow at the European Centre on Privacy and Cybersecurity at the University of Maastricht, where he co-leads the Humanitarian Action Programme.

Aaron Martin is an Assistant Professor of Media Studies and Data Science at the University of Virginia, United States. His research interests include data governance in development and humanitarian contexts, critical infrastructure protection, surveillance, and biometrics.

Olivier Matter is the Head of International Cooperation within the Policy and Consultation Unit of the European Data Protection Supervisor (EDPS). He coordinates the involvement of the EDPS in the activities of the European Data Protection Board and leads its Key Provisions Expert Subgroup. Before joining the EDPS, he worked for the Council of Europe, at the *Commission Nationale de l'Informatique et des Libertés*, and as a data protection lawyer.

Hiroshi Miyashita is a Professor of Law (LL.D.), Faculty of Policy Studies, Chuo University in Japan. His academic interests include constitutional law and data protection law.

Cosimo Monda is the Director of the European Centre on Privacy and Cybersecurity at Maastricht University. His fields of expertise include Data Protection and Cybersecurity; EU Information Management; Transparency and Access to Documents; EU Agencies; EU decision-making procedures and Institutions, and EU law.

Silvia Pelucchi is the Data Protection Outreach Coordinator at the International Committee of the Red Cross, where she has worked across various departments for more than seven years. She specialises in data protection in humanitarian action, leading training, outreach, and research initiatives while promoting internal awareness of the responsible use of data and technology.

Emrys Schoemaker is the Director of Policy & Advisory at Caribou Digital (United Kingdom). He is a senior research fellow at the Graduate Institute, Geneva, where he coordinates the Digital Sovereignty Observatory. His expertise and research interests include digital transformation, infrastructures, and governance in development and humanitarian contexts.

Martin Searle is the Director of Analysis at *Médecins Sans Frontières*, Hong Kong. He specialises in migration, technology, and humanitarian engagement in China and Southeast Asia.

Cassie Jiun Seo is a humanitarian aid professional specialising in digital interventions in humanitarian aid worker working at the intersection of technology and the public interest. Her experience includes roles with the Norwegian Refugee Council and the World Health Organisation. She also conducts research on humanitarian technology practices at the MCTD, University of Cambridge.

Cristina Teleki is an Assistant Professor at the European Centre on Privacy and Cybersecurity, working on the regulation of Big Tech. She earned her doctoral degree at Bern University (Switzerland), focusing on the right to a fair trial in EU competition law.

Quito Tsui is a researcher and writer focused on technology use in the humanitarian and development sectors. She leads the Humanitarian AI + MERL Working Group at the MERL Tech Initiative where she is a core collaborator.

Jean-Philippe Walter is the Data Protection Commissioner (until the end of June 2025), a member of the International Committee of the Red Cross Data Protection Commission, former Deputy Federal Data Protection Commissioner (Switzerland), former Chairman of the Association *francophone des autorités de protection des données*, and former Chairman of the Consultative Committee of Convention 108.

Betty (Jia Li) Wang is an Associate Innovation Officer at the United Nations High Commissioner for Refugees, spearheading the Connectivity for Refugees initiative. She brings experience from previous roles at Deloitte, Collective Aid, and the World Economic Forum.

John Warnes is a Senior Innovation Officer at the United Nations High Commissioner for Refugees. His expertise focuses on connectivity, digital economic inclusion, and digital protection of forcibly displaced people. He has an LLM in IT Law and Telecommunications from the University of Southampton.

Wojciech Wiewiórowski is the European Data Protection Supervisor. Before his appointment, he served as Assistant European Data Protection Supervisor, as Inspector General for the Protection of Personal Data at the Polish Data Protection Authority, and as Professor at the Faculty of Law and Administration of the University of Gdańsk.

FOREWORD

Wojciech Wiewiórowski

Contemporary humanitarian action increasingly relies on the processing of vast information resources – primary and secondary data collection, analysis, and exchange. A significant portion of this data is linked to specific individuals: aid beneficiaries, aid workers, or intermediaries. Where once physical presence and goodwill were sufficient, today information systems, the identification of aid beneficiaries, and a precise mapping of their needs are necessary. In this dynamic environment, the underlying question of the book you hold in your hands becomes more and more pressing: *"How do we effectively protect the personal data of the people we want to help?"*

Processing the personal data of refugees, victims of conflict or natural disasters carries enormous risks. Such data can become a tool of oppression or discrimination. Humanitarian organisations and other actors involved must therefore not only provide assistance, but also act responsibly and in accordance with principles stemming from law, the internal arrangements of international organisations, and the ethics of data processing.

We all seem to know what humanitarian action is. It comprises organised efforts to help people affected by natural disasters, armed conflicts, refugee crises, epidemics, and other emergencies that threaten life, health, safety, or human dignity. However, we are not fully aware of the practical challenges of carrying out humanitarian operations, particularly those that extend beyond the jurisdiction of a single state.

When I first encountered the topic of data protection and privacy in humanitarian action, serving as assistant European Data Protection Supervisor

(EDPS) at the time, I simply approached it as yet another field – or sector – of social activity in which we implement the same data protection and privacy principles, perhaps with some specificities.

How wrong I was!

Working for several years as a lawyer and for more than four years as a national data protection supervisor in Poland, I had become accustomed to working with various charities, public administrations, law enforcement agencies, and the military dealing with natural disasters and catastrophes. Humanitarian actions in the EU and humanitarian actions organised in the remotest regions of the world have the same goal – to save lives and alleviate suffering. However, they differ significantly in terms of context, scale, resources, and types of needs. In EU countries, humanitarian action most often occurs in response to natural disasters (e.g. floods, fires, pandemics), mass influxes of refugees, or social crises. In Europe's neighbouring Africa, humanitarian actions in response to armed conflict, famine, epidemics, drought, lack of infrastructure, and structural poverty are far more prevalent.

Differences in infrastructure relate not only to hospitals, roads, emergency services, transport, health care, and clean water, but also – very significantly – to IT infrastructure and the internet. The differences are not always about the level of infrastructural development. For example, differences in the role of mobile internet in Africa and Europe, or differences in ownership of networks on the two continents, can result in the need to build quite different logistical and legal structures for humanitarian action.

In countries subject to the EU General Data Protection Regulation (GDPR), most crises and actions are of a short-term nature, which encourages various types of short-term derogations and special measures for data processing. More attention is paid to ensuring the temporary nature of these measures, the erasure of data resources created on an *ad hoc* basis, and the evaluation of the performance of the system, while of course taking care to protect the 'essence' of the rights to privacy and data protection. These are usually the jurisdictions where civil law and specific branches of law – such as constitutional law or administrative law – can assist as well. In different regions of the world, humanitarian actors must often take into account that many measures will be long-term, humanitarian, and developmental at the same time – and that the assistance will often last for years.

I learned all these truths, which I should have already known before, from Massimo Marelli – one of the co-editors of this book – and from the group of experts who contributed to the Handbook on Data Protection in Humanitarian Action, the first edition of which was published in 2015. I also learned from them and from other experts in the context of the workshops dedicated to data protection with international organisations which are

co-organised, on a regular basis, by the EDPS. These workshops, initiated in 2005, are an opportunity for all international organisations to exchange their experiences and views on the most pressing issues they are facing. Over the years, the relevance and significance of these workshops have grown consistently. This confirms the need for this platform for international organisations to engage, share best practices, and discuss common challenges, as well as increasing awareness of the importance of protecting individuals' personal data around the world.

Today, after two decades of promoting data protection in humanitarian action together, experts in the field, law, technology, crisis management, and ethics share their knowledge and experience with us. They analyse real cases, point out best practices, and caution against mistakes. Together, we consider how to build trust in extreme situations, where data protection may not be a luxury, but a foundation. This book is an invitation to reflect on how to combine operational effectiveness with respect for human dignity.

Undoubtedly, there is much to discuss and write about. As humanitarian organisations target various – sometimes very distant – regions of the world, one has to acknowledge that the protection of personal data poses a number of legal, technological, and ethical challenges. One of the greatest risks is the potential for data security breaches. In situations of armed conflict or humanitarian crises, information can end up in the wrong hands – e.g. of armed groups or repressive regimes. This can lead to persecution, discrimination, and even violence against aid beneficiaries. In addition, humanitarian organisations are increasingly becoming targets of cyber attacks because they store sensitive data, such as information on health status, ethnicity, religion, or refugee status.

The variety of legal frameworks is another major challenge. Organisations operating internationally have to adapt to the legal systems of different countries, such as the GDPR in the European Union or the Health Insurance Portability and Accountability Act in the United States. The lack of consistent data protection standards in many countries is also an issue, even today when most countries in the world theoretically have comprehensive data protection laws in place. Actual protection, however, does not boil down to just the letter of the law.

The collection of personal data in crisis situations exacerbates the challenges encountered. Faced with the lack of stable technical infrastructure, data has to be collected anyway – often in a hurry, without fully informing those affected. The trust of the people affected is the foundation of effective humanitarian action. However, many people, especially refugees, may be distrustful of having their data collected, especially if they have had traumatic experiences with authorities. Moreover, there is sometimes a need for rapid intervention – using, for example, medical data – which can present further challenges. Collaborating and sharing data with partners such as the United

Nations, local non-governmental organisations, or state institutions can also be a challenge.

In conclusion, responsible data management in the humanitarian sector requires not only robust technological safeguards, but also ethical sensitivity, knowledge of the law, and measures that promote trust among the communities being helped. Only then is it possible to provide support that truly protects rather than puts at risk those most in need.

The authors of this book are the heroes of this difficult daily struggle for data protection in conflict zones or politically unstable states, which involves risks not only for the people targeted by humanitarian action but also for the humanitarian workers themselves. They have to work with local leaders, informal structures, and sometimes with authorities with – to put it mildly – limited legitimacy, from whom accountability cannot be exacted and who will certainly want to become data controllers.

The privacy and data protection professionals contributing to this book promote adherence to data protection standards in organisations that are sometimes the only real source of support for local populations. In their work, they keep in mind that the key characteristics of humanitarian action are neutrality (aid is provided without taking sides in a conflict), impartiality (aid goes to all those in need, regardless of nationality, religion, gender, or opinion), humanitarianism (the main objective is to save lives and alleviate suffering), and independence (humanitarian organisations act autonomously from governments and political groups).

Let's embark on a journey to uncover the fruits of their labour.

ACKNOWLEDGEMENTS

This book is a collaborative effort initiated by the Data Protection Office at the International Committee of the Red Cross (ICRC), the Data Protection Office at the UN High Commissioner for Refugees (UNHCR), and the Global Privacy Assembly (GPA) and particularly its Working Group on the Role of Privacy in International Development Assistance, International Humanitarian Assistance and Crisis Management (WG AID).

It began small with a special triple anniversary of these three organisations – the 10th year anniversaries of the establishment of the ICRC Data Protection Framework, the adoption of the UNHCR Policy on the Protection of Personal Data of Persons of Concern, and the adoption of the GPA Resolution on Privacy and International Humanitarian Action. Yet, it has blossomed into a broader, shared vision that takes stock of the progress made by the entire humanitarian sector over the past decade and charts a course for the decade to come.

We would like to begin by expressing our deepest gratitude to UNHCR, especially Alex Novikau, and to the GPA, particularly Catherine Lennman, for their invaluable partnership, dedication, and expertise.

It has been a genuine privilege to collaborate with the many co-authors who curated the 20 chapters of this volume, bringing together a rich and diverse range of perspectives from academia, policy, and practice in data protection and the humanitarian sector: Ana Beduschi, Romain Bircher, Dogu Han Buyukyagcioglu, Stuart Campo, Gilles Cerutti, Timothy

Charlton, Florence Dubosc, David Erdos, Julia Feigen, Larissa Fast, Emily Knox, Natalie Klein-Kelly, Sophie Kwasny, Catherine Lennman, Charlotte Lindsey, Aaron Martin, Cosimo Monda, Hiroshi Miyashita, Silvia Pelucchi, Cassie Jiun Seo, Emrys Schoemaker, Martin Searle, Cristina Teleki, Quito Tsui, Christina Vasala Kokkinaki, Jean-Philippe Walter, John Warnes, Betty (Jia Li) Wang, and Wojciech Wiewiórowski et al. Their exceptional dedication and ability to produce such high-quality work under tight, seemingly impossible deadlines, have been truly inspiring and are an important testament to the joint engagement on a shared mission, driven by a commitment to impact and a will to help contribute to the constant improvement of humanitarian action for the benefit of those who need it most. We are deeply grateful for their remarkable contributions and the positive impact they have made on the entire volume.

This volume benefited greatly from the contributors' workshop held at the University of Cambridge (UK). We are thankful to the contributors, respondents, peer reviewers, and advisory board members, who generously contributed their time and expertise during the workshop. Our special thanks are due to the Minderoo Centre for Technology & Democracy, particularly Gina Neff and Christine Adams, as well as to Wolfson College, with special appreciation to its president, Dame Ijeoma Uchegbu, and to Jamie Trinidad, for generously hosting this event and providing the platform for rich exchanges that significantly shaped this volume.

The progress of this volume was expertly guided by a distinguished Advisory Board, enriched by the outstanding group of respondents at the Cambridge workshop, and further refined through a rigorous peer review. We are profoundly grateful to all Advisory Board members, peer reviewers, and respondents who donated their time and expertise.

The Advisory Board comprises:

- Immaculate Kassait, Data Commissioner at the Office of the Data Protection Commissioner in Kenya;
- Christopher Kuner, Affiliate Professor at the University of Copenhagen, Senior Privacy Counsel at Wilson Sonsini Goodrich & Rosati;
- Catherine Lennman, Chair of the WG AID of the GPA, delegate for International Affairs and Francophonie of the Swiss Office of the Federal Data Protection and Information Commissioner (FDPIC);
- Gina Neff, Executive Director of the Minderoo Centre for Technology & Democracy at the University of Cambridge;
- Alex Novikau, Chief Data Protection Officer at UNHCR;
- Carmela Troncoso, Scientific Director at the Max Planck Institute for Security and Privacy in Bochum, Germany.

The peer reviewers comprise:

- Stuart Campo, Senior Impact Advisor at the International Organization for Migration (IOM);
- Davide Cascone, Data Protection Legal Advisor at the ICRC;
- Pierrick Devidal, Senior Policy Advisor at the ICRC;
- Ben Hayes, Independent consultant at UN Human Rights Office;
- Kristin Bergtora Sandvik, Professor at the University of Oslo;
- Philippe Stoll, Digital technologies and armed conflicts;
- Linnet Taylor, Professor at Tilburg University.

The respondents at the Cambridge workshop comprise:

- Dogu Han Buyukyagcioglu, Data Protection Officer at the UNHCR;
- Stuart Campo, Senior Impact Advisor at the International Organization for Migration (IOM);
- Pierrick Devidal, Senior Policy Adviser at the ICRC;
- David Erdos, Professor at the University of Cambridge;
- Ben Hayes, Independent consultant at UN Human Rights Office;
- Claire Jervis, Legal Consultant and Researcher at Data Protection Matters;
- Chiara Manfredini, EU Policy Associate at Access Now;
- Olivier Matter, Team Leader for International Cooperation at the European Data Protection Supervisor (EDPS).

We would also like to acknowledge the European Centre on Privacy and Cybersecurity (ECPC) at Maastricht University, not only for their valuable contributions to the chapters of this volume but also for their generous institutional support. Aaron Martin would like to thank the Robert Bosch Stiftung Foundation for its financial support.

Many thanks to Routledge Publishing, especially Alison Kirk, and the managing editorial team, Maria Haas, Silvia Pelucchi, and Jie Yang, for their professionalism and efficiency in bringing this book to reality within a compressed timeframe. We also appreciate Paul Garwood, our copyeditor, for his meticulous attention to detail, which significantly enhanced the quality of this volume.

For many years, our efforts in advancing data protection in humanitarian action have been made possible thanks to the unwavering and generous support of the Luxembourg Ministry of Foreign Affairs and the Swiss Federal Department of Foreign Affairs. Much of what is captured in this book could not have been achieved without their partnership, commitment, and trust over the past decade.

This volume exists also because of the tireless dedication of countless humanitarian workers. Daily, often in the most challenging of circumstances,

they uphold the principles of humanity, independence, impartiality, and neutrality. As eloquently expressed by Wojciech Wiewiórowski in the foreword, it is through their unwavering commitment that the vision of safeguarding data protection and protecting the dignity of affected individuals carries on into the future. This book, therefore, also carries our deepest gratitude to them.

Finally, to all readers, within and beyond the humanitarian and data protection fields, thank you for engaging with this book. Your attention helps underscore the urgent need for society to confront the growing challenges of privacy and data protection in humanitarian action.

Let us embark together on the next decade's odyssey to strengthen data protection in humanitarian action.

– Ana Beduschi, Massimo Marelli, Aaron Martin

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Introduction

DATA PROTECTION IN HUMANITARIAN ACTION

Responding to Crises in a Data-Driven World

Ana Beduschi, Massimo Marelli, and Aaron Martin

Introduction

In 2015, ten years ago, the Directorate of the International Committee of the Red Cross (ICRC) adopted its first comprehensive Rules on Personal Data Protection (the Rules).[1] This marked a significant institutional milestone, providing the ICRC, an organisation with a status equivalent to that of an international organisation,[2] with a dedicated regulatory framework on personal data protection. The Rules integrated globally accepted data protection principles and requirements, informed by key legal developments of that time, including those emerging through the negotiations of the EU General Data Protection Regulation (GDPR)[3] and of the Council of Europe's Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108+).[4] They also created a supervisory body, the ICRC Data Protection Office (DPO), and a

1 ICRC, "ICRC Rules on Personal Data Protection" (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

2 See Els Debuf, "Tools to do the job: The ICRC's legal status, privileges and immunities," *International Review of the Red Cross* 97, no. 897–898 (2015): 319–344: https://international-review.icrc.org/sites/default/files/irc_97_1-2-13.pdf.

3 European Parliament and Council, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ L 119, 4 May 2016, 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

4 Council of Europe (CoE), *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Treaty, Council of Europe Treaty Series (CETS), No. 223, Strasbourg, 10 October 2018: https://rm.coe.int/16808ac918.

DOI: 10.4324/9781003650164-1

mechanism for ensuring effective remedies for individuals with complaints about the handling of their personal data through the establishment of a Data Protection Commission at the level of the ICRC Assembly.[5]

In the same year, the Office of the United Nations High Commissioner for Refugees (UNHCR) also adopted its own regulatory framework on personal data protection with the introduction of its Policy on the Protection of Personal Data of Persons of Concern to UNHCR.[6] The policy reflected a longstanding human rights-based approach, establishing safeguards for the collection, use, and sharing of personal data, including that of displaced individuals, donors, and partners. It has since been expanded through the General Policy on Personal Data Protection and Privacy (GDPP),[7] which brings the organisation's practices in line with modern and global standards. The GDPP established the role of a Chief Data Protection Officer to provide independent oversight and guidance, and introduced a formal review mechanism for complaints, reinforcing transparency, accountability, and trust in UNHCR's data processing activities.

That same year, the Global Privacy Assembly (GPA, then the International Conference of Data Protection and Privacy Commissioners), a global forum bringing together data protection and privacy authorities from more than 130 countries,[8] adopted the Resolution on Privacy and International Humanitarian Action,[9] marking the first time humanitarian action was formally recognised within a global forum of data protection and privacy regulators. The resolution acknowledged the growing reliance on personal data in humanitarian crises and called for greater cooperation with humanitarian actors, recognising their unique mandates and operational contexts. It also established a dedicated Working Group on Privacy and Humanitarian Action, tasked with developing guidance that would support rather than hinder principled humanitarian work. The resolution thus laid a foundation for sustained engagement between the humanitarian and data protection communities, and for the development of standards tailored to humanitarian realities.

5 "The ICRC data protection framework," ICRC, 2 June, 2020, https://www.icrc.org/en/document/icrc-data-protection-framework.

6 "Data protection," UNHCR, accessed 16 June, 2025, https://www.unhcr.org/what-we-do/reports-and-publications/data-and-statistics/data-protection.

7 UNHCR, General Policy on Personal Data Protection and Privacy (GDPP), 2022, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207.

8 https://globalprivacyassembly.org/.

9 International Conference of Privacy and Data Protection Commissioners, *Resolution on Privacy and International Humanitarian Action*, 37th International Conference, Amsterdam, 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

In the years since, the humanitarian landscape has continued to evolve, with digital technologies becoming deeply embedded in humanitarian action. Today, these technologies play a central role in how needs are assessed and how humanitarian programmes are delivered. From real-time data collection for needs assessments,[10] to beneficiary registration and management in aid programmes through digital identity systems,[11] digital tools have become integral to the daily operations of humanitarian organisations, reshaping how they carry out their work.

Yet this digital transformation has also brought significant challenges. Increased connectivity, complex data flows, and growing reliance on third-party service providers have made it more difficult to uphold the transparency, agency, and accountability that principled humanitarian action requires.

This shift has had profound implications, both for affected populations and for humanitarian organisations themselves. First, it has made it significantly more challenging to ensure the respect of the rights and dignity of individuals in humanitarian contexts. Dignity is closely tied to a person's ability to retain agency and some degree of control over information about themselves – a challenging prospect even in stable settings, but one made much more difficult in situations of displacement, vulnerability, disempowerment, and crisis. Second, the digital transformation has placed new pressures on the operating modalities of humanitarian organisations. As third-party service providers play an increasingly prominent role in humanitarian data processing, risks of surveillance and data repurposing threaten the neutrality, impartiality, independence, and the exclusively humanitarian nature of humanitarian participants' actions. It also threatens, as a consequence, the trust that is the precondition for humanitarian access, accessibility, and acceptance.

In the face of these challenges, data protection has emerged not only as a matter of regulatory compliance, but as a key enabler of principled humanitarian action. Its contributions to the sector lie not just in legal safeguards: data protection frameworks also offer practical tools for mapping and managing

10 For example, drones, or unmanned aerial vehicles (UAVs), can provide high-resolution imagery for damage assessment, mapping disaster zones, and locating displaced populations, while crowdsourcing can help analyze this data to enhance situational awareness and humanitarian response planning. See Marelli ed., *Handbook on Data Protection in Humanitarian Action*, Chapter 7.

11 For instance, the WFP's SCOPE platform facilitates beneficiary registration and aid management by integrating biometric authentication to enhance efficiency and accountability, while UNHCR's Biometric Identity Management System (BIMS) enables real-time identity verification across operations using fingerprints and iris scans. See, "WFP SCOPE," *WFP*, https://usermanual.scope.wfp.org/cash-accounts/content/common_topics/introduction/1_introduction.htm, and "Planning and Preparing Registration and Identity Management Systems: 3.6 Registration Tools," *UNHCR*, https://www.unhcr.org/registration-guidance/chapter3/registration-tools/.

risks, strengthening transparency, and embedding accountability, all while reinforcing the neutrality, independence, impartiality, and the exclusively humanitarian nature on which humanitarian action depends.

To capture the complexity of this evolving landscape, and the contribution of data protection law and practice to humanitarian action, this edited volume brings together a range of perspectives – academic analyses, policy reflections, and personal experiences from humanitarian practitioners – each offering a distinct but complementary lens on the role of data protection in humanitarian action. The themes addressed across the volume are deliberately varied yet deeply interconnected. From operational challenges and regulatory cooperation to local perspectives, cross-sector partnerships, and responsible data-sharing, each chapter reflects on the contribution of data protection to the daily practice and strategic evolution of humanitarian work, drawing on multiple disciplines and experiences.

The volume comprises five interconnected sections, designed to provide a comprehensive understanding of data protection in the humanitarian sector. In Section 1, Chapter 1 by Marelli provides context and a conceptual framework for the volume, outlining the many challenges common to the sector and reflecting on ten years of data protection in humanitarian action.

Section 2 explores the transformation of the humanitarian space. The first subsection, 2.1, examines the evolving humanitarian environment, specifically focusing on how rapid increases in connectivity for crisis-affected communities have expanded the scale of responsibility for protecting personal data, as discussed by Warnes and Wang in Chapter 2. In Chapter 3, Bircher presents a personal account that highlights the challenges of building secure digital humanitarian platforms such as the ICRC's RedSafe initiative. Additionally, Chapter 4 by Tsui examines how biometric technologies have reshaped organisational accountability structures. The second subsection 2.2 explores the digital transformation of the humanitarian space through the lens of data protection itself. In Chapter 5, Schoemaker and Martin discuss how digital public infrastructure and data protection considerations are reshaping the humanitarian-development nexus. In Chapter 6, Searle and Lau analyse the implications of digitalisation and hyper-connectivity for humanitarian independence. Lindsey, in Chapter 7, explores how data protection can serve as a foundational pillar for trusted digital transformation in humanitarian contexts.

Section 3 addresses the complex intersection of data protection with international law, diplomacy, and humanitarian practice. The first subsection 3.1 examines the evolution of legal frameworks, opening with Chapter 8, where Erdos revisits the foundational 1990 UN Guidelines on Personal Data Regulation and their continued relevance for international humanitarian organisations. In Chapter 9, Vasala Kokkinaki explores the legal tensions between EU data protection laws and the privileges and immunities of UN

system organisations. Walter and Kwasny, in Chapter 10, examine the role of Convention 108+ for international organisations, while Lennman and Dubosc, in Chapter 11, investigate how the GPA contributes to regulatory cooperation in humanitarian contexts. The second subsection 3.2 offers contributions reflecting on practical applications of data protection in humanitarian action. In Chapter 12, Knox analyses data protection in family links restoration services, a core activity for the International Red Cross and Red Crescent Movement, while Klein-Kelly, in Chapter 13, reflects on the lessons learned from the 2022 data breach affecting the Family Links Network. In Chapter 14, Buyukyagcioglu questions the maturity of understanding regarding data protection in humanitarian practices. Fast, Campo and Cerutti examine in Chapter 15 the complex dynamics of responsible data sharing between humanitarian organisations and their donors.

Section 4 shifts the focus to community-based and regional perspectives in data protection. Charlton and Seo analyse in Chapter 16 how data protection legislation is reshaping humanitarian action and data subject rights in Ukraine. In Chapter 17, Charlton, Feigen, and Pelucchi examine the factors influencing perceptions of data collection and processing in humanitarian settings. The section concludes with Chapter 18, in which Miyashita reflects on the data protection challenges specific to the Asia-Pacific region, highlighting how cultural, political, and legal traditions shape approaches to humanitarian data governance.

Finally, Section 5 looks towards the future. Monda and Teleki examine in Chapter 19 how data protection education and training can serve as a trust-building mechanism in the humanitarian sector. Chapter 20 by Wiewiórowski et al. offers an analysis of the implications of artificial intelligence for humanitarian data protection. This chapter considers how the humanitarian sector may build capacity while addressing emerging technological challenges through a framework of digital humanism that prioritises human dignity and agency.

The various contributions in this volume collectively demonstrate that data protection has become indispensable to humanitarian action in the digital age. However, they also reveal significant gaps and challenges that require ongoing attention. Looking ahead, the contributors identify several key areas for future development, notably the need to strengthen frameworks for responsible innovation that prioritise human dignity and uphold humanitarian principles. The volume also emphasises the importance of continued dialogue between humanitarian practitioners, data protection experts, academia, and the affected communities themselves. By bringing together diverse perspectives and experiences, this volume aims to contribute to a more nuanced and effective approach to data protection in the humanitarian context – one that recognises both the promise and the perils of the data-driven age.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

PART 1

Setting the Scene

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1

THE CONTRIBUTION OF DATA PROTECTION TO HUMANITARIAN ACTION

Ten Years of Data Protection in Humanitarian Action

Massimo Marelli[1]

Introduction

As digital technologies and data-driven approaches reshape the humanitarian landscape, the responsible handling of personal data has become central to safeguarding the rights and dignity of affected people. While these tools can enhance the reach, speed, and efficiency of the humanitarian response, they also introduce new risks, operational complexities, and ethical dilemmas. In this evolving context, data protection offers more than just legal safeguards: it provides a critical lens to navigate these challenges and ensure that digital transformation supports, rather than undermines, humanitarian objectives. This chapter sets the stage by examining the drivers of this transformation and the growing role of data protection as both a safeguard and an enabler of responsible humanitarian action.

The chapter begins by examining humanitarian action in the digital age, tracing the drivers and dynamics of the sector's digital transformation, and the growing centrality of data. It then shows how data protection has evolved in parallel, becoming increasingly vital to navigating these changes. The discussion highlights two major impacts of these developments: first, the heightened challenges of upholding the dignity, rights, and agency of affected populations in increasingly data-driven environments (and how data protection enables a more transparent, accountable, and context-sensitive response); and second, the growing risks linked to third-party access and the erosion

1 The opinions and views expressed in this article are the author's own and do not necessarily represent those of the ICRC. Special thanks go to Maria Haas for her input and research support. All errors are the author's own.

DOI: 10.4324/9781003650164-3

of trust in humanitarian operations (and how data protection reinforces the legal and operational safeguards humanitarian actors rely on). Finally, the chapter looks ahead, identifying the capacities, partnerships, and innovations required to ensure that the sector's digital transformation remains responsible, principled, and fit for humanitarian purpose.

By weaving together these developments, this chapter provides the context and analytical foundation for understanding the role of data protection in today's humanitarian landscape – and how it continues to evolve as both a safeguard and enabler of responsible and accountable humanitarian action.

Humanitarian Action in an Era of Digital Transformation

Over the past decade, digital transformation has significantly reshaped the humanitarian sector. Across industries, the early 2010s were marked by a wave of digital innovation and a culture of experimentation, often driven by a desire to "move fast and break things".[2] While this mindset originated outside the humanitarian sphere, it gradually influenced the sector, accelerating the adoption of digital tools and data-driven approaches to enhance the delivery of aid and protection.

But the shift towards digital is not merely the result of hype. It has been driven by a combination of factors particularly relevant for the humanitarian sector: the rapid expansion of digital connectivity among affected populations, the need to respond to increasingly complex and protracted crises, the coexistence and overlap between humanitarian action and development and social protection systems, and growing expectations for more efficient and accountable aid. Together, these drivers have made digital infrastructure and systems central to humanitarian action, creating new opportunities but also introducing new risks.

With data at the heart of these developments, data protection has grown in relevance and maturity. It has evolved in parallel with the sector's digital transformation, offering a structured framework to navigate the legal, operational, and ethical complexities of humanitarian work in an increasingly data-driven world.

2 The phrase "Move fast and break things" was the internal motto used by Facebook until 2024, popularised by founder Mark Zuckerberg and embodying a mindset of rapid innovation, continuous experimentation, and a willingness to disrupt the *status quo*. See, for example, Jordan Liles, "Did Mark Zuckerberg Say, 'Move Fast And Break Things'?" Snopes, 29 July 2022, accessed 13 February 2025, https://www.snopes.com/fact-check/move-fast-break-things-facebook-motto/.

Data: At the Heart of Humanitarian Action

At the heart of humanitarian action lies its commitment to people: to prevent and alleviate human suffering wherever it may be found. Rooted in its fundamental principles, particularly the principle of humanity, humanitarian work is driven by the objective to protect life and health and to ensure respect for the human being.[3]

Today, data plays a crucial role in enabling that mission. Reliable data, especially personal data, is widely seen as essential to the effective design and delivery of humanitarian operations. It can support needs assessments during humanitarian emergencies and help ensure that humanitarian services are effectively designed, tailored, monitored, and adapted to changing circumstances and needs. In principle, data can enable humanitarian organisations to be more responsive, adaptive, and effective in their interventions. For example, tracking supply chains can ensure that food and water reach disaster-affected areas without delay. In conflict zones, personal data can facilitate secure access to lifesaving information, such as evacuation routes or medical assistance. Additionally, collecting and sharing personal data enables humanitarian organisations to register displaced persons, reunite families, and provide targeted aid, ensuring that services are tailored to the evolving needs on the ground.[4]

However, in the humanitarian sector, personal data is never just a tool. Each data set represents real people's experiences, often coupled with their suffering, a community's needs, or a crisis unfolding in real time. When used responsibly, data can amplify the voices of those affected, guiding humanitarian actors in delivering more targeted and effective responses.

Digital Transformation in Humanitarian Action Beyond the Hype: Drivers and Dynamics

As technology advances, digital transformation has emerged as a response to the sector's need to adapt to new realities on the ground, the evolving nature of humanitarian crises, opportunities offered by technological advances, and the growing and evolving needs and expectations of affected populations, donors, and humanitarian workers. Before turning to the important risks and

3 See, for example, the preamble to the *Statutes of the International Red Cross and Red Crescent Movement*. Adopted 2006, 5, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/statutes-en-a5.pdf.

4 See, for example, "At the Intersection of Humanitarian Action and Cyberspace," *ICRC*, 11 February 2025, https://www.icrc.org/en/article/symposium-intersection-humanitarian-action-and-cyberspace.

challenges raised by digital transformation and technology in the humanitarian sector, this section maps out some of these key drivers and dynamics.

The Humanitarian Sector in the Age of Digital Disruption

The mantra of "move fast and break things" from the early 2010s became a hallmark of the cultural shift in the digital landscape, which sparked a wave of digital innovation and experimentation and drove various sectors towards risk-seeking trial-and-error approaches to achieve breakthrough progress.[5]

This mindset – of moving quickly, embracing failure as a learning opportunity, and innovating on the go – which mirrored broader trends across industries, began trickling into the humanitarian sector. With this shift, humanitarian organisations started to embrace digital transformation and integrate digital tools and data-driven solutions at a much faster pace, inspired by the potential of new technologies to improve the way aid and protection were delivered.[6]

The humanitarian sector is not immune, however, to the risks of technological hype, where new tools and approaches are sometimes promoted more for their novelty than for their actual effectiveness in addressing humanitarian needs.[7]

Yet, the digital shift in humanitarian action has not been driven by fleeting hype alone. In fact, there are several compelling incentives for adopting digital services in humanitarian action which have driven digital transformation in the sector, as illustrated below.

Firstly, as noted, humanitarian work is driven by the fundamental principle of humanity, the focus of which is to prevent and alleviate human suffering wherever it may be found, protect life and health, and ensure respect for the human being.[8] When new technologies and tools have the potential to enhance the efficiency and effectiveness of humanitarian interventions, potentially allowing humanitarian organisations to do more and reach further, engaging with them, understanding them, and, *where appropriate*, embracing them becomes a moral responsibility.

5 Liles, "Did Mark Zuckerberg Say, 'Move Fast And Break Things'?".

6 UN Office for the Coordination of Humanitarian Affairs (OCHA), *From digital promise to frontline practice: new and emerging technologies in humanitarian action*, April 2021, https://reliefweb.int/report/world/digital-promise-frontline-practice-new-and-emerging-technologies-humanitarian-action.

7 See, for example, Dzhennet-Mari Akhmatova and Malika-Sofi Akhmatova, "Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype," *Journal of International Humanitarian Action* 5, no. 1 (June 2020), https://doi.org/10.1186/s41018-020-00076-2.

8 Preamble to the *Statutes of the International Red Cross and Red Crescent Movement*, 5.

This approach is also complemented by a commitment to donors and stakeholders who expect accountability, transparency, and the efficient use of resources.[9] The integration of some digital solutions has the potential to enable humanitarian organisations to meet the evolving needs of affected communities, but also ensures that donor expectations are met by improving the effectiveness and reach of interventions.

Secondly, pervasive and expanding internet access has become a reality in many parts of the world. While this may still not be the case everywhere,[10] over the past ten years, crisis-affected communities have experienced unprecedented growth in digital connectivity, enabling faster and broader communication and increased flows of personal data. By the end of 2023, 4.6 billion people worldwide, 57% of the global population, were using mobile internet, a significant leap from 33% in 2015.[11] This number is projected to reach 5.5 billion by 2030.[12] This rapid expansion in digital access brings with it both opportunities and heightened expectations for the humanitarian sector to be responsive and adapt to a more connected world.[13] In fact, as digital access is rising, so is access to digital services, and people in crises expect humanitarian organisations to provide services through digital channels.[14] Similarly, humanitarian workers themselves are coming to expect modern digital tools to support and enhance their operations.[15]

With this growing reliance on mobile technology and heightened expectations, humanitarian aid has moved beyond traditional forms of support like

9 See, for instance, UN High Commissioner for Refugees (UNHCR), *Digital Transformation Strategy 2022–2026*, 27, https://www.unhcr.org/digitalstrategy/wp-content/uploads/sites/161/2023/07/Digital-Transformation-Strategy-2022-2026-UNHCR-Web.pdf.

10 In some of the ICRC's largest operations, including, for instance in Sudan, mobile internet access remains limited, reaching just 29.3% of the population in 2023, up only slightly from 26.1% in 2013. This disparity underscores the need for a context-specific approach to digital engagement and connectivity planning in humanitarian response. See, Global System for Mobile Communications Association (GSMA), "The State of Mobile Internet Connectivity Report 2024," accessed 24 February 2025, https://www.gsma.com/r/somic/.

11 GSMA, "The State of Mobile Internet Connectivity Report 2024".

12 GSMA, "The Mobile Economy 2025," https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/02/030325-The-Mobile-Economy-2025.pdf.

13 See, for instance, UNHCR, *Digital Transformation Strategy 2022–2026*, 22–23.

14 UNHCR Innovation Service, *Connecting With Confidence: Managing Digital Risks to Refugee Connectivity*, 46, https://www.unhcr.org/innovation/wp-content/uploads/2021/03/CWC-Managing-Digital-Risks-To-Refugee-Connectivity-Report.pdf. For earlier reports on this phenomenon, see ICRC, The Engine Room, and Block Party, "Humanitarian Futures for Messaging Apps," January 2017, https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

15 See, for instance, UNHCR, *Digital Transformation Strategy 2022–2026*, 32.

food, shelter, and water and sanitation.[16] Digital connectivity is now seen as vital, enabling people to communicate, access information, and exercise their rights, such as reconnecting with loved ones or applying for asylum.[17]

Building on this enhanced connectivity, humanitarian organisations are increasingly able to offer digital platforms and services that cater to the evolving needs and considerations of affected populations, making aid and protection more accessible and responsive. One notable example is RedSafe, developed by the International Committee of the Red Cross (ICRC). Having been designed with the objective of ensuring the privacy and safety of its users, RedSafe illustrates how digital connectivity can empower populations in vulnerable situations by providing them with the tools to access essential services more securely and effectively. The experience of designing it and deploying it with these objectives also provides a good illustration of the challenges of building user-centric technology in humanitarian settings, and of the meaning and modalities of implementing data protection by design in these contexts.[18]

The Changing Nature of Humanitarian Crises and the Need for Digital Proximity

A third reality that the humanitarian sector must face is the increasingly complex, protracted, and fragmented nature of humanitarian crises, particularly in situations of conflict and violence. Conflicts today tend to last longer than in the past,[19] fluctuate between periods of high and low intensity over a protracted time, leading to unprecedented levels of humanitarian need.[20] The number of people in need of humanitarian assistance has soared, from an estimated 78 million in 2015 to just shy of 300 million in 2024, according

16 Rakesh Bharania and Mark Silverman, "Protective by Design: Safely Delivering Connectivity as Aid," *Humanitarian Law & Policy Blog* (blog), 8 July 2021, https://blogs.icrc.org/law-and-policy/2021/07/08/protective-by-design-connectivity-as-aid/.

17 Connectivity today is seen both as a tool for humanitarian action ("connectivity for aid") and as a vital service that people in crises increasingly rely on ("connectivity as aid"). As digital access expands, the need to safeguard and provide connectivity grows, with its absence potentially having serious humanitarian consequences. See, for instance, Massimo Marelli, *Handbook on Data Protection in Humanitarian Action*, Chapter 16; and Kimberly Brown, "Connectivity and mobile technology: A humanitarian lifeline," *TechForGood*, 10 February 2025, https://www.techforgood.net/thoughtleadership/connectivity-and-mobile-technology-a-humanitarian-lifeline.

18 For further discussion, see Chapter 3, "The challenges of building RedSafe, a secure digital humanitarian platform. An unsafe journey?".

19 "Protracted conflict," *International Review of the Red Cross*, no. 912 (November 2019), https://international-review.icrc.org/reviews/irrc-no-912-protracted-conflict.

20 OCHA, *From digital promise to frontline practice: new and emerging technologies in humanitarian action*.

to the United Nations Office for the Coordination of Humanitarian Affairs' (OCHA) annual Global Humanitarian Overview.[21]

Longer-lasting conflicts require continued support over extended periods, often involving repeated distribution of assistance rather than isolated interventions. This, in turn, raises the risks of duplication, inefficiencies, and possibly fraud.[22] In this context, digital tools such as biometric technologies and identity management systems have come to be viewed as helpful assets for humanitarian organisations to improve identification accuracy, reduce fraud, and enhance accountability across operations.[23]

Periods of lower conflict intensity often see humanitarian action intersecting more directly with state-led protection systems and development aid programmes, necessitating coordination between *ad hoc* humanitarian responses and more institutionalised, long-term approaches, as discussed below.[24]

At the same time, many conflicts today are shaped by highly fragmented stakeholder environments with unclear hierarchies, often involving non-state actors, radical groups, or splinter factions.[25] This fragmentation complicates the ability of humanitarian organisations to identify and engage the right interlocutors and provide humanitarian access, which depends on dialogue and acceptance by all relevant parties. In such environments, digital tools, such as data analytics and artificial intelligence (AI), have been identified as

21 OCHA, *Global Humanitarian Overview 2015*, 8 December 2014, https://www.unocha.org/publications/report/world/global-humanitarian-overview-2015 and OCHA, *Global Humanitarian Overview 2024*, 11 December 2023, https://www.unocha.org/publications/report/world/global-humanitarian-overview-2024-enarfrsp.

22 ICRC, *Protracted Conflict and Humanitarian Action*, August 2016, https://www.icrc.org/sites/default/files/document/file_list/protracted_conflict_and_humanitarian_action_icrc_report_lr_29.08.16.pdf.

23 OCHA, *From digital promise to frontline practice: new and emerging technologies in humanitarian action*, and Vincent Graf Narbel and Justinas Sukaitis, "Biometrics in Humanitarian Action: A Delicate Balance," *Humanitarian Law & Policy Blog* (blog), 2 September 2021, https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/. An example of the use of such a tool is UNHCR's Biometrics Identity Management System (BIMS), which enhances identification accuracy and helps prevent fraud across operations. See "Planning and Preparing Registration and Identity Management Systems: 3.6 Registration Tools," UNHCR, https://www.unhcr.org/registration-guidance/chapter3/registration-tools/. For further discussion, see also Chapter 4 "The logic of biometrics and organisational accountability".

24 See, for instance, Ellen Policinski and Jovana Kuzmanovic, "Protracted Conflicts: The enduring legacy of endless war," *International Review of the Red Cross*, no. 912 (November 2019), https://international-review.icrc.org/articles/protracted-conflicts-enduring-legacy-endless-war-ir912.

25 Hichem Khadhraoui, "Fragmentation of armed non-State actors in protracted armed conflicts: Some practical experiences on how to ensure compliance with humanitarian norms," *International Review of the Red Cross*, no. 912 (November 2019), https://international-review.icrc.org/articles/fragmentation-armed-non-state-actors-protracted-armed-conflicts-ir912.

opportunities to support situational awareness by monitoring and analysing large volumes of data, including from traditional and social media, to help identify emerging risks and opportunities for engagement.[26]

Against this backdrop, digital tools and technologies have come to be seen as important enablers of effective humanitarian action. At their best, they can ensure that responses are not only immediate but also sustained, coordinated, and people-centric.[27] With better access to more data, organisations can track and analyse needs more accurately, leading to earlier, faster, and more targeted responses. For example, digital cash transfers offer rapid, flexible assistance aligned with the actual needs of affected populations,[28] while AI, when properly designed, can help detect patterns in complex humanitarian data to support forecasting and operational planning.[29]

Beyond optimising needs assessments and aid delivery, digital tools also enable humanitarian workers to maintain communication with communities in remote or insecure areas, helping ensure the continuity of services while also enhancing staff safety and security. In this context, therefore, the integration of both physical and digital proximity is critical.[30] While a physical presence often remains indispensable for establishing the trust necessary to provide aid and protection, digital proximity has emerged as a necessity in modern humanitarian responses. By combining both physical and digital proximity, humanitarian organisations can operate more efficiently, better support people in hard-to-reach areas, while better protecting those working on the ground.

The Overlap and Coexistence Between Humanitarian Action and Social Protection

A fourth key force shaping the digital transformation of the humanitarian sector is the evolving relationship between humanitarian action and social

26 Marelli ed., *Handbook on Data Protection*, Chapters 14 and 17.

27 OCHA, *From digital promise to frontline practice: new and emerging technologies in humanitarian action*.

28 Jo Burton, "'Doing No Harm' in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action," *International Review of the Red Cross* 102, no. 913 (April 2020): 43–73, https://doi.org/10.1017/S1816383120000491, and Marelli ed., *Handbook on Data Protection*, Chapter 9.

29 Ana Beduschi, "Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks," *International Review of the Red Cross* 104, no. 919 (April 2022): 1149–1169, https://doi.org/10.1017/S1816383122000261.

30 Massimo Marelli, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation," *International Review of the Red Cross* 102, no. 913 (April 2020): 369, https://doi.org/10.1017/S1816383121000151.

protection systems, particularly in fragile environments.[31] In these contexts, humanitarian needs fluctuate significantly, and the response mechanisms must adapt to cycles of acute crises and relative stability. This has fuelled increasing efforts to align humanitarian action with longer-term development strategies, with the goal of creating more sustainable and predictable support structures.

One of the most prominent initiatives in that area is the Grand Bargain, which seeks to integrate humanitarian, development, and peace efforts to ensure that aid reaches those in need more effectively.[32] The push for such integration at an infrastructural level rather than on an *ad hoc* basis is often framed as a means to enhance efficiency, effectiveness, and sustainability.[33] However, this transition also carries significant implications with it. Digital systems initially designed for short-term emergency response, such as cash transfers, digital identity frameworks, and biometric verification, are then expected to operate within long-term development and state-run social protection frameworks. This shift assumes a degree of interoperability between systems built for different purposes, under different governance models, and with varying levels of legal oversight.[34]

As a result, a critical challenge in this nexus is the growing overlap between humanitarian digital infrastructure and national or international social protection systems. While development-oriented social protection schemes prioritise universal access and long-term inclusion, humanitarian action is guided by principles of independence, neutrality, and impartiality, which, in turn, require that data collected for humanitarian purposes remains used exclusively for humanitarian purposes, and does not end up being used for purposes that may be incompatible with these fundamental principles. The increasing pressure to integrate these systems, therefore, raises concerns about possible "scope creep" where technologies originally designed for emergency relief are repurposed or used for other purposes, potentially undermining humanitarian mandates.[35]

31 Cristina Quijano Carrasco, "Humanitarian Engagement in Social Protection: Implications for Principled Humanitarian Action," *Humanitarian Law & Policy Blog* (blog), 11 February 2021, https://blogs.icrc.org/law-and-policy/2021/02/11/humanitarian-engagement-social-protection/.

32 The Grand Bargain is an agreement between humanitarian donors and aid organisations, launched at the World Humanitarian Summit in May 2016. See "The Grand Bargain (Official website)," *Inter-Agency Standing Committee (IASC)*, accessed 14 February 2025, https://interagencystandingcommittee.org/grand-bargain.

33 See, for instance, Victoria Metcalfe-Hough, Wendy Fenton, and Farah Manji, *Grand Bargain Annual Independent Report 2023*, IASC, https://interagencystandingcommittee.org/grand-bargain-official-website/grand-bargain-annual-independent-report-2023-0.

34 For further discussion, see Chapter 5, "Digital transformation and the humanitarian-development transition: the role of Digital Public Infrastructure and data protection".

35 Bert-Jaap Koops, "The concept of function creep," *Law, Innovation and Technology* 13, no. 1 (2021): 29–56. https://doi.org/10.1080/17579961.2021.1898299.

Moreover, digital infrastructure that supports humanitarian response often operates outside national frameworks.[36] As such infrastructure becomes more embedded within national social protection systems, questions arise about control, data governance, and the risk of unintended consequences. The push for greater interoperability must therefore be weighed against the need to preserve a principled digital space – one that safeguards the independence, neutrality, and impartiality of humanitarian organisations and ensures that data remains confined to its exclusively humanitarian purpose, as discussed below.

The Implications of Digital Transformation: New Challenges for the Humanitarian Sector

As the humanitarian sector embraces digital transformation, the arguments around possible benefits of improved efficiency and expanded reach are compelling and full of promise. However, the potential of these advancements comes with an equally significant expansion of risk surface, for both the people whose data is collected, and for the humanitarian organisations leveraging these technologies. The increasing reliance on digital tools, ranging from biometric registration to mobile cash transfers and other digital services, has dramatically amplified the volume and granularity of data generated and used in crisis contexts. At the same time, these tools rely on increasingly complex data flows and a growing ecosystem of third-party service providers that often operate outside the direct oversight of humanitarian actors.

Increased Digital Footprints and the Complexity of Data Flows

One of the most pressing concerns brought by the digital transformation is the exponential expansion of digital footprints for both affected populations and humanitarian organisations. Individuals seeking assistance and protection often engage with digital tools that collect, store, and share data across multiple systems – whether through mobile money transfers, health databases, or communications over messaging apps.

The increase in digital interactions, be it for communication and outreach, cash and fund transfers, or case management, has also led to highly intricate data flows. Humanitarian organisations must navigate a complex network of data processing operations, potentially involving third parties such as cloud

36 For further discussion, see Chapter 8, "Legal tensions: insights from the UN-EU correspondence on EU data protection law and the role of privileges and immunities as a catalyst for enhancing personal data protection".

service providers,[37] financial institutions,[38] telecommunications companies,[39] and governmental regulators.[40] This may give rise to critical situations where data collected by a humanitarian organisation for exclusively humanitarian purposes, secured through its privileges and immunities in the case of an international organisation (IO),[41] could end up being processed by third parties acting under a separate legal regime. This growing interconnectivity[42] makes it increasingly difficult to conduct thorough risk assessments, ensure proper data governance, and maintain oversight of where data is stored, processed, transferred to, and for what purposes, thereby further eroding accountability and agency, and increasing risks for data subjects.

Moreover, there is metadata associated with these interactions, such as timestamps, locations, and devices used, which can offer third parties detailed insights into individual behaviour and interactions, even without direct access to the content. This unintended exposure of sensitive metadata, often without the individual's knowledge or consent, further exacerbates the risk of surveillance and exploitation. These will be further explored below.[43] This digital footprint is not only vast but also highly revealing, making individuals more susceptible to profiling, monitoring, and exploitation.

37 See, for example, Marelli ed., *Handbook on Data Protection*, Chapter 10.

38 See, for example, Marelli ed., *Handbook on Data Protection*, Chapter 9, and ICRC and Privacy International, "The Humanitarian Metadata Problem," Chapter 6.

39 See, for example, Marelli ed., *Handbook on Data Protection*, Section 12.2.1.1 and ICRC and Privacy International, "The Humanitarian Metadata Problem," Chapter 5.

40 See, for example, Marelli ed., *Handbook on Data Protection*, Chapter 11.

41 Massimo Marelli, "The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads Between the International and Domestic Legal Orders," *Computer Law and Security Review* 50 (2023), https://doi.org/10.1016/j.clsr.2023.105849. See also, Explanatory Statement No. 5 of International Conference of Privacy and Data Protection Commissioners, *Resolution on Privacy and International Humanitarian Action*, 37th International Conference, Amsterdam, 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf; and "Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection," Resolution (33rd International Conference of the Red Cross Red Crescent Movement, December 2019), https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

42 See Chapter 13, "Data protection and independence in an age of hyperconnectivity".

43 For elaboration on these issues, see also ICRC and Privacy International, "The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era," October 2018, https://www.icrc.org/sites/default/files/document/file_list/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

The Increasing Reliance on Third-Party Service Providers in Humanitarian Action

In today's digital world, the delivery of humanitarian efforts is undergoing a fundamental paradigm shift. Humanitarian programmes are no longer built solely on traditional bilateral relationships between humanitarian organisations and affected populations. Instead, they increasingly depend on a vast and complex network of external processors and sub-processors, including telecommunications companies, cloud service providers, financial institutions, and social media platforms.[44]

These third-party actors – along with their regulators – increasingly govern key aspects of humanitarian data processing and storage, often beyond the direct oversight of humanitarian organisations. As humanitarian organisations increasingly rely on third-party digital infrastructure, the humanitarian sector must now contend with a web of intermediaries that not only contributes to the complexity of data flows, as described above, but also comes with its own commercial or profit-making drivers, data management policies, security vulnerabilities, regulatory oversight or surveillance, and regulatory obligations. As a result, humanitarian data is increasingly exposed to a broader ecosystem of interests that may not (fully) align with humanitarian principles and working modalities.

Together, these developments have reshaped the landscape in which humanitarian organisations operate, creating not only new possibilities but also new pressures. Two major impacts have emerged from this shift: first, on the ability to uphold the rights, dignity, and agency of affected populations; and second, on the operating modalities of humanitarian organisations, particularly their ability to preserve the exclusively humanitarian character of their work. These will be examined in more detail below.

The Data Protection Lens: Responding to the Challenges of Digital Transformation

In response to these changes, data protection has emerged over the last ten years as a central operational and ethical consideration for humanitarian actors. With data now at the heart of how humanitarian programmes are designed and delivered, humanitarian organisations have increasingly recognised the need for structured, principled approaches to managing digital risks and upholding the dignity and rights of those they serve.

The following sections trace this evolution: first, by outlining the rights-based foundations of data protection and how they resonate with humanitarian principles; and second, by showing how the sector has committed to

44 See, for instance, Marelli ed., *Handbook on Data Protection*, Section 4.1.

these principles and translated them into concrete safeguards and institutional frameworks.

Understanding Data Protection: A Rights-Based Approach

At its core, data protection is an area of law based on rights. The origins of modern data protection are rooted in Convention 108, the first legally binding international treaty to regulate the automatic processing of personal data. Adopted by the Council of Europe on 28 January 1981, Convention 108 was groundbreaking in establishing common legal principles to safeguard individuals' fundamental rights in the face of increasing computerisation and digitalisation. Recognising the growing role of information and communication technologies (ICT) in data processing, the Convention set out to ensure that personal data would be handled in a lawful, fair, and transparent manner, irrespective of national borders.[45]

The right to privacy, enshrined in Article 8 of the European Convention on Human Rights (ECHR),[46] laid the foundation for Convention 108, recognising privacy as a cornerstone of human dignity and democratic societies. But data protection extends beyond the right to privacy. It embeds principles such as data minimisation, purpose limitation, and security safeguards to prevent the exploitation of personal information. The EU Charter of Fundamental Rights[47] further strengthened this understanding by explicitly articulating and distinguishing between the right to privacy (Article 7) and the right to data protection (Article 8), affirming the latter as a distinct and enforceable right.

Since then, these rights have been reinforced and expanded through key legal instruments such as the EU Data Protection Directive[48] and the EU

45 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, 28 January 1981, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. One of the Convention's most notable contributions was its technological neutrality, allowing its principles to remain relevant despite rapid advancements in digital tools and data-driven processes. See also Urszula Góral, *The right to privacy and the protection of personal data: Convention 108 as a universal and timeless standard for policymakers in Europe and beyond* (2021), https://doi.org/10.18276/ais.2021.33-06.

46 Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14. Rome*, 4 November 1950, European Treaty Series – No. 5.

47 European Union, *Charter of Fundamental Rights of the European Union*, OJ C 326, 26 October 2012, 391–407, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2012_326_R_0391_01.

48 European Parliament and Council, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of*

General Data Protection Regulation (GDPR).[49] These instruments can be seen as manifestations of the obligations that EU Member States have under Convention 108. All EU Member States are parties to the Convention and are bound under international law to implement a protective data framework in line with its principles.[50] The GDPR, in this context, can be seen as the expression of this commitment within the EU legal order.

Over the decades, Convention 108 has become the backbone of global data protection law, influencing national legislation not only across the Council of Europe area but also well beyond, including countries in Latin America, Africa, and Asia.[51] In 2018, its modernised version, Convention 108+,[52] was introduced to address contemporary challenges, enhancing accountability mechanisms, individual rights, and safeguards to ensure that data protection remains a core element of human rights protection in the digital age.[53]

It follows that the core of data protection, being about the respect of the rights and dignity of individuals when data relating to them is collected and used, aligns intrinsically with the foundational values of humanitarianism. The principle of upholding human dignity and integrity, one of the core commitments of humanitarian efforts and of the fundamental principle of humanity, finds a natural counterpart in data protection's grounding in dignity[54] and emphasis on fairness, transparency, and purpose limitation. Just as humanitarian action is guided by the imperative to prevent harm and protect those in crisis, data protection serves to limit harmful consequences that may result from handling people's data. In this way, it reinforces the humanitarian commitment to the principle of "Do No Harm", not only in physical interventions, but also in the digital realm.[55]

---

personal data and on the free movement of such data, OJ L 281, 23 November 1995, 31–50, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

49 European Parliament and Council, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ L 119, 4 May 2016, 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

50 https://www.coe.int/en/web/data-protection/convention108/background.

51 "From Europe to the World: The EU and Council of Europe as Global Standard Setters in Data Protection," *European External Action Service (EAAS)*, 28 January 2021, https://www.eeas.europa.eu/eeas/europe-world-eu-and-council-europe-global-standard-setters-data-protection_en.

52 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

53 For further discussion, see Chapter 9, "Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+) and international organisations".

54 See para. 3 of the Preamble to Convention 108+.

55 The principle of "Do No Harm", also known as the "humanitarian imperative", stipulates that humanitarian efforts must avoid causing adverse impacts or the creation of new risks

The Evolution of Data Protection in Humanitarian Action: A Turning Point in 2013–2015

Over recent decades, data protection has experienced very significant growth as an area of law, evolving in response to increasing concerns over the involvement of third-party service providers, the complexity of data flows, digital dependence, and the risk, especially, of commercial exploitation. These concerns, which are particularly acute in humanitarian contexts, have driven the sector towards more structured and principled approaches to data protection.[56]

A defining moment in this evolution came with the Snowden revelations in 2013, which exposed the global scale of bulk and non-targeted data collection conducted by intelligence agencies.[57] This revelation, according to some observers, brought additional focus and momentum to the European data protection debate. While the GDPR does not, and could not, address the substance of the data collection practices in question, this focus was instrumental in both shaping the GDPR into a landmark legal framework that prioritises individual rights, accountability, and strict data processing conditions, and in leading to its final adoption.[58]

This period, which was characterised by a focus on data protection rights and the adoption of the GDPR, also marked a turning point for the humanitarian sector, with civil society observers starting to highlight the risks that new technologies deployed by humanitarian organisations posed to the rights, and especially the privacy rights, of the people they were meant to protect and assist.[59] It is at this point and in this context that the ICRC and the UN Refugee Agency (UNHCR) adopted their first comprehensive regu-

---

for individuals and populations, and it applies not only to physical interventions but also to digital operations. See, for instance, Mary B. Anderson, "Do No Harm: How Aid Can Support Peace or War," *International Journal on World Peace* 16, no. 3 (1999): 85–87; Kristin Bergtora Sandvik, Katja Lindskov Jacobsen, and Sean Martin McDonald, "Do no harm: A taxonomy of the challenges of humanitarian experimentation," *International Review of the Red Cross* 99, no. 1 (2017): 319–344, https://international-review.icrc.org/articles/do-no-harm-taxonomy-challenges-humanitarian-experimentation; and Hugo Slim, *Humanitarian Ethics: A Guide to the Morality of Aid in War and Disaster* (Oxford University Press, 2015).

56 For further discussion, see Chapter 14, "Growing data protection maturity in humanitarian action: changes in understanding of key concepts in theory and in practice".

57 "Edward Snowden: Leaks that exposed US spy programme," *BBC*, 17 January 2014, https://www.bbc.com/news/world-us-canada-23123964.

58 Agustín Rossi, "How the Snowden Revelations Saved the EU General Data Protection Regulation," *The International Spectator* 53, no. 4 (November 13, 2018): 95–111, https://doi.org/10.1080/03932729.2018.1532705.

59 A landmark in this sense was the 2013 Privacy International report on "Aiding Surveillance – An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries," http://privacyinternational.org/report/841/aiding-surveillance.

latory frameworks in the area of personal data protection. In 2015, the ICRC adopted the ICRC Rules on Personal Data Protection (the Rules),[60] and UNHCR its General Policy on Personal Data Protection and Privacy (the Policy).[61]

To support and ensure the application of this framework, the ICRC's Data Protection Office (DPO) was established in 2015 to facilitate and monitor the application of the Rules, reinforce institutional accountability, and enable the organisation to adapt to an increasingly complex data landscape. Finally, the ICRC Data Protection Commission was also established in the same year as an independent body of the ICRC Assembly, and granted decision-making powers that are binding on the organisation to ensure that an effective remedy is available to data subjects in case of breaches of the Rules.[62] Through initiatives such as the Restoring Family Links (RFL) Code of Conduct,[63] advocacy in global policy discussions, and other integral policies and guidelines, such as the Policy on the Processing of Biometric Data,[64] the ICRC has attempted to address the intersection between humanitarian action, digital transformation, and data protection, ensuring that legal safeguards are not only aligned with international standards but also serve the realities of humanitarian work. These issues will be explored below, where the discussion focuses on how data protection serves as a tool for addressing the realities of humanitarian contexts.

As such, data protection maturity in the humanitarian sector has grown and evolved over the years,[65] and data protection has become a fundamental pillar of humanitarian operations. The next section explores how this imperative plays out in practice: in efforts to ensure respect for the dignity, agency, and rights of individuals affected by crises in an increasingly digitalised operational environment.

60 ICRC, "ICRC Rules on Personal Data Protection," (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

61 UNHCR, *General Policy on Personal Data Protection and Privacy (GDPP)*, 2022, Article 18, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207.

62 "The ICRC data protection framework," *ICRC*, 2 June 2020, https://www.icrc.org/en/document/icrc-data-protection-framework.

63 For further discussion, see Chapter 11, "Data protection in the framework of Restoring Family Links humanitarian activities: Code of conduct, resolutions, and data breaches".

64 The Policy on the Processing of Biometric Data outlines both technical and legal safeguards to ensure that sensitive biometrics data is handled with integrity and respects the rights and dignity of individuals. See ICRC, *Policy on the Processing of Biometric Data by the ICRC*, adopted 28 August 2019, https://www.icrc.org/sites/default/files/document/file_list/icrc_biometrics_policy_adopted_29_august_2019_.pdf.

65 For further discussion, see Chapter 14, "Growing data protection maturity in humanitarian action: changes in understanding of key concepts in theory and in practice".

Impact on the Capacity to Ensure Respect of the Rights and Dignity of Affected Populations

The first major impact of the landscape described above concerns the ability to ensure respect of the rights and dignity of affected persons whose data is processed. The digital transformation of humanitarian action has introduced new layers of complexity that make this core humanitarian imperative increasingly difficult to fulfil. Fragmented data ecosystems, limited visibility of data flows, and the growing involvement of multiple third parties have weakened the conditions under which individuals can meaningfully exercise agency or influence how their personal data is used.

Yet it is precisely in humanitarian settings, where people are often displaced, disempowered, and dependent on external assistance, that retaining some element of agency and control over personal data becomes most critical.

In this context, data protection emerges as more than a regulatory requirement. It provides concrete contributions to safeguarding dignity and rights in the face of these challenges. It offers risk assessment tools that help reintroduce visibility and accountability, and allows for a contextualised application of its principles to reflect the operational realities of humanitarian crises. Together, these dimensions help establish the conditions under which dignity, agency, and accountability can be meaningfully upheld.

Agency, Control, and Dignity in the Midst of Disempowerment

The first major impact of the evolving digital humanitarian landscape is its disruptive effect on the ability of humanitarian actors to ensure respect of the rights and dignity of individuals when processing their personal data. Important elements of dignity are linked to a person's capacity to retain agency and some element of control over what happens to the intimate information about themselves and their relationships, who sees it, and for what purpose it is used.

This capacity is difficult to guarantee even in stable settings. But it becomes significantly more precarious in humanitarian contexts, where individuals are often thrust into extreme vulnerability. Displacement, loss of belongings, separation from family members, and breakdowns in access to justice or social support structures are common.[66] In such environments, the ability to make autonomous decisions is already severely diminished. Individuals' destinies may rest in the hands of conflict actors or armed groups, while their survival and wellbeing often depend on the assistance provided by humanitarian organisations.

66 See, for instance, the ICRC's approach to understanding the experiences of internally displaced people, https://www.icrc.org/en/document/internally-displaced-people.

In this setting, humanitarian actors become not only providers of aid but also gatekeepers of access, protection, and information. Individuals must entrust them not only with their immediate needs but also with sensitive personal data, often without valid alternatives. This creates an acute form of disempowerment that makes it all the more important to preserve whatever agency and control individuals can retain, particularly over their personal information.

Retaining agency in such contexts means being able to understand and influence what data is collected, how it is used, and by whom. It also requires mechanisms of accountability: ensuring that those who hold power over this data are answerable to those whom it concerns. But digital transformation has introduced new dynamics that make this extraordinarily difficult. Complex data ecosystems – often involving multiple third-party service providers, cloud platforms, financial institutions, and regulators – have transformed what was once a bilateral relationship into a fragmented web of actors, as discussed *supra* in relation to the growing reliance on third-party service providers in humanitarian action. In many cases, data collected by humanitarian organisations is processed across borders or under separate legal regimes, reducing the visibility and control that both organisations and individuals can exercise.[67]

In this context of compounded vulnerability and diffuse data control, ensuring the dignity and rights of affected individuals requires more than good intentions. It demands a deliberate and structured approach to guaranteeing agency, visibility, and accountability.

Data Protection as a Tool for Enabling Transparency and Accountability

In this context, data protection emerges not merely as a legal obligation, but as a practical framework to help reintroduce visibility, restore a degree of control, and build trust in increasingly complex and opaque humanitarian data environments. Designed to safeguard individual rights in digital environments, data protection brings structure to contexts that are otherwise fragmented and disempowering, especially for those whose lives depend on the services of humanitarian actors.

One of the most important contributions of data protection in this context is its emphasis on risk-based thinking. Before risks can be mitigated, they must first be understood. Data protection principles require humanitarian organisations to conduct systematic assessments of how personal data is processed, by whom, and for what purpose. This starts with mapping data flows and identifying all the actors involved, including third-party service providers,

67 Marelli, "The Law and Practice of International Organisations' Interactions with Personal Data Protection Domestic Regulation".

sub-processors, and regulators – often across borders and subject to domestic legislation.[68]

Tools like Data Protection Impact Assessments (DPIAs) are not simply compliance exercises; they help uncover where vulnerabilities lie, clarify the roles and responsibilities of each actor, and make visible risks that might otherwise remain hidden.[69]

The ability to map and assess data flows becomes especially important in humanitarian contexts, where data often crosses borders, legal regimes, and institutional boundaries. This raises additional challenges for IOs, which must ensure the continuity of data protection across these environments. Data protection frameworks also offer mechanisms to facilitate such cross-border transfers responsibly – though the legal and institutional dimensions of these mechanisms are explored in detail elsewhere.[70]

This visibility of risks is key to restoring accountability, both internally, by ensuring that humanitarian organisations take responsibility for data practices across their operations, and externally, by enabling affected individuals to know who is using their data and for what ends. In contexts where agency is already compromised, this form of structural transparency becomes essential. Without it, affected individuals are reduced to data subjects in systems they cannot see or influence.

Importantly, these data protection tools and principles directly support humanitarian organisations in meeting their commitments to Accountability to Affected Persons (AAP).[71] AAP is not just about communicating with communities, but about ensuring that organisations are answerable to the people they serve, especially when digital systems mediate their access to services, protection, or even recognition. In an environment characterised by interdependent actors, fast-evolving technologies, and blurred jurisdictional

68 See, for example, Marelli ed., *Handbook on Data Protection*, Chapter 11, which outlines how domestic laws in various jurisdictions may require service providers to disclose humanitarian data, such as communications, metadata, or beneficiary information, to State authorities for purposes of national security or criminal proceedings. These laws often apply irrespective of humanitarian mandates, and without explicit humanitarian exemptions, posing serious implications for neutrality, independence, and operational security.

69 See Marelli ed., *Handbook on Data Protection*, Chapter 5.

70 See, for instance, Massimo Marelli, "Transferring personal data to international organisations under the GDPR: an analysis of the transfer mechanisms," *International Data Privacy Law* 14, no. 1 (2023): 19–36, https://doi.org/10.1093/idpl/ipad022. See also Marelli, "The Law and Practice of International Organisations' Interactions with Personal Data Protection Domestic Regulation".

71 For more on AAP, see, for instance, UNHCR, "Accountability to Affected People (AAP)," Emergency Handbook, https://emergency.unhcr.org/protection/protection-principles/accountability-affected-people-aap.

boundaries, data protection provides a grounding framework for making AAP operational.[72]

In this way, data protection does more than shield individuals from harm: it equips humanitarian actors to act with clarity and integrity in complex digital environments. It helps restore the conditions under which agency, dignity, and accountability can meaningfully be upheld.

Data Protection as a Tool for Addressing the Realities of Humanitarian Contexts

Another feature that makes data protection particularly valuable to humanitarian action is also its adaptability. One of its strengths lies in enabling a contextualised application of its principles and requirements, which is particularly valuable in exceptional environments such as humanitarian crises, where rigid application of standard rules may undermine rather than protect the rights and dignity of affected individuals.

Humanitarian settings present certain specificities that have significant implications for how data protection principles are interpreted and applied in these circumstances. These specificities must be carefully considered in order to ensure that the regulatory frameworks applied in such extreme circumstances are fit for purpose and capable of achieving their fundamental objective – namely, the meaningful protection of the rights and dignity of data subjects.

This need for contextualised application of data protection standards in humanitarian settings has been acknowledged in various international instruments. Most notably, the UN General Assembly's Guidelines for the Regulation of Computerized Personal Data Files[73] (1990) (the UN Guidelines) include a "humanitarian clause", which explicitly recognises the need for tailored application of data protection principles and requirements in service of humanitarian aims, "when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance".[74]

72 For an example of the operationalisation of these principles, see ICRC, *Accountability to Affected People Institutional Framework*, January 2020, https://www.icrc.org/en/publication/accountability-affected-people-institutional-framework.

73 UN General Assembly. *Resolution 45/95: Guidelines for the Regulation of Computerized Personnel Data Files,* 14 December 1990, UN Doc. A/RES/45/95, https://digitallibrary.un.org/record/105299?v=pdf.

74 See para. 6, https://www.refworld.org/policy/legalguidance/unga/1990/en/13761. The humanitarian clause authorises departure from the principle of lawfulness and fairness (Principle 1), the principle of accuracy (Principle 2), the principle of the purpose-specification

By embedding humanitarian considerations in a UN soft law instrument, the clause provided early international recognition of and legitimacy to the need for specific adaptations and derogations for humanitarian purposes and laid the groundwork for data protection standards in the humanitarian sector. The Resolution on Privacy and International Humanitarian Action adopted by the 37th International Conference of Privacy and Data Protection Commissioners in 2015 notably refers back to the humanitarian clause, reaffirming its importance and drawing attention to the need for a specific interpretation and application of data protection principles in humanitarian contexts.[75]

These foundational recognitions paved the way for a growing body of work exploring how data protection frameworks can be meaningfully applied to the evolving realities of humanitarian action. As digital transformation accelerates, new and complex challenges have emerged, and the data protection lens of analysis has become an essential tool for identifying underlying risks, understanding their implications, and developing context-sensitive ways to navigate them. The section that follow each highlight a different area where this analytical framework has helped humanitarian actors navigate the operational, legal, and ethical dimensions of digital transformation.

Beyond Consent: Ensuring Lawfulness and Fairness

One widely recognised example of the need for contextualised application of data protection principles relates to the key requirements of lawfulness and fairness in data processing.[76] Under data protection frameworks, any processing of personal data by a data controller must be grounded in a valid legal basis that legitimises it. Humanitarian organisations have traditionally regarded consent as the primary, if not the only, means of legitimising the collection and processing of personal data.[77] However, the unique nature of

(Principle 3), and the principle of interested-person access (Principle 4) if necessary to protect the rights and freedoms of others, particularly in humanitarian situations.

75 See the preamble to the International Conference of Privacy and Data Protection Commissioners, *Resolution on Privacy and International Humanitarian Action*, 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

76 See, for instance, Marelli ed., *Handbook on Data Protection*, Chapter 3; Centre for Information Policy Leadership, *The Limitations of Consent as a Legal Basis for Data Processing in the Digital Society* (2024), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_bkl_limitations_of_consent_legal_basis_data_processing_dec24.pdf; or ICRC, *Professional Standards for Protection Work*, 4th ed., (2024): 108–112, https://shop.icrc.org/professional-standards-for-protection-work-pdf-en.html.

77 See, for instance, the first edition of the ICRC *Professional Standards for Protection Work* (2009), which states that "Protection actors must only collect personal information with the informed consent of the person concerned, who is made aware of the purpose of the

humanitarian contexts has increasingly highlighted the limitations of relying on consent to ensure that people retain meaningful control, and the importance of considering alternative legal bases that may better reflect the operational realities on the ground.

For consent to be valid, it must be specific, freely given, informed, and unambiguous – criteria that are inherently difficult to fulfil in humanitarian contexts.[78] Several factors contribute to this challenge. First, individuals affected by humanitarian emergencies, particularly those linked to armed conflict and violence, face additional and enhanced elements of vulnerability. This vulnerability stems not only from their unstable and precarious circumstances but also from the fact that some data subjects may be unconscious, missing, or otherwise unable to fully appreciate and take a position as to the implications of data collection and processing.[79]

Second, the urgent and immediate nature of humanitarian needs often places individuals in a position of dependency on humanitarian aid and protection. This often results in a power imbalance between affected individuals and the humanitarian organisations seeking to provide protection and assistance to them, which can leave individuals with limited choice, making it difficult to ensure that consent for sharing their data is truly free.

Compounding these challenges is the complexity of data processing in humanitarian operations, particularly when advanced technologies such as biometrics are involved. Meaningful consent requires individuals to understand the risks and implications of data collection, but the complexity of these systems can make it difficult for individuals, limiting their ability to make truly informed decisions. In fact, in fast-moving crises, data may be processed in ways that even humanitarian organisations sometimes struggle to fully anticipate.[80] When data flows through digital infrastructure involving multiple actors, such as cloud providers, financial institutions, or government agencies, the ability of any individual to assess potential risks and consequences is severely limited.

---

collection" (64–65), https://globalprotectioncluster.org/sites/default/files/2022-09/b0687fcbbbd8e82e852576810057e6be-icrc-protectionstandards-nov2009.pdf. The IOM *Data Protection Manual* (2010) similarly emphasises that consent should always be obtained, unless "exceptional circumstances hinder the achievement of consent" (11), https://publications.iom.int/books/iom-data-protection-manual. The ICRC *Rules of Personal Data Protection*, in their 2015 and 2019 versions, also referred to consent as the "preferred basis for processing personal data" (Article 1.3). This reference was removed in the 2025 revision of the Rules.

78 Marelli ed., *Handbook on Data Protection*, Section 3.2.

79 Marelli ed., *Handbook on Data Protection*, Section 3.2.

80 See, for instance, Andrea Düchting, *Humanitarian Topics explained: Digitalisation in humanitarian action to go*, (2024): 10, https://www.chaberlin.org/wp-content/uploads/dlm_uploads/2024/07/cha-digitalisation-in-humanitarian-action-to-go-en.pdf.

The unique combination of these factors renders consent often unsuitable as a legal basis for processing personal data in humanitarian settings. International, domestic, and institutional data protection frameworks have recognised these challenges and offer viable alternatives to consent to ensure that data processing remains lawful and fair. These notably include the vital interest of the data subject or another person, which allows data processing when necessary to protect life, dignity, or security,[81] and the public interest legal basis, which permits processing where it is necessary for the performance of a humanitarian mandate established under national or international law.[82]

For example, Recital 46 of the GDPR explicitly states that processing personal data may be justified by the need to protect an individual's vital interests in emergency situations or for compelling public interest reasons, including for humanitarian purposes.[83] Similarly, Convention 108+, in its Explanatory Report,[84] and the Updated Principles on Privacy and Personal Data Protection of the Organization of American States (OAS)[85] highlight the importance of allowing data processing based on vital and public interest grounds in humanitarian settings.

Beyond these international frameworks, the regulatory frameworks of international organisations also reflect this approach. The ICRC's Rules on Personal Data Protection,[86] UNHCR's Policy on Personal Data Protection and Privacy,[87] the World Health Organization's (WHO) Personal Data Protection Policy,[88] and the UN Children's Fund's (UNICEF) Policy on Personal Data Protection[89] all provide for alternative legal bases that could be

81 Examples include searching for missing persons, identifying human remains, providing medical care, and responding to imminent threats.

82 This is applicable to international organisations active in the area of humanitarian action such as the ICRC, UNHCR, UNICEF, WFP, and IOM, or to national organisations such as National Societies of the Red Cross and Red Crescent, or non-governmental organisations with which a specific task of public interest is agreed upon with the authorities with responsibility for this task.

83 In fact, Recital 46 states: "Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters".

84 See para. 67 of the Explanatory Report to Convention 108+.

85 OAS, *Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with Annotations* (Inter-American Juridical Committee, 8 April 2021): 34 and 74.

86 ICRC, *ICRC Rules on Personal Data Protection*, Article 1.3.

87 UNHCR, *General Policy on Personal Data Protection and Privacy (GDPP)*, 2022, Article 18.

88 WHO, *Personal Data Protection Policy*, 2024, Article 2.1.

89 UNICEF, *Policy on Personal Data Protection*, 2020, para. 15.

more appropriate than consent, recognising the necessity of processing data in the vital or public interest when fulfilling humanitarian mandates.

This principle has also been endorsed in important international instruments and fora. The 2019 Resolution on Restoring Family Links while respecting privacy (RFL Resolution), for instance, explicitly acknowledges the need to process personal data within the International Red Cross and Red Crescent Movement (the Movement) for humanitarian purposes, and recognises both public interest and vital interest as essential legal bases for data processing in situations where consent is neither practical nor appropriate.[90]

Together, these frameworks underscore that data protection is not merely a compliance requirement but a crucial enabler of lawful, accountable, and legitimate data processing in humanitarian contexts. By providing a number of alternatives that can be used instead of consent to reflect the realities of crisis contexts, and combining them with elements of responsibility and accountability, data protection frameworks enable humanitarian action all while ensuring the rights and dignity of individuals.

The Sensitive Nature of Data in Humanitarian Contexts

Another specific challenge in applying data protection principles in humanitarian contexts relates to the nature of the data involved. Data protection laws generally afford specific protection to certain categories of data, often referred to as sensitive or special categories of data, and provide that these types of data can only be processed under narrowly defined conditions. This relates to the processing of data which, depending on context, could result in significant risks to the fundamental rights and freedoms of the data subjects.[91] While the rationale for providing specific protection and restrictions on the handling of data is grounded in contextual risk, some legal frameworks, such as the GDPR in Article 9, provide closed lists of types of data that fall under this category.

In humanitarian settings, however, such fixed classifications often fall short. The sensitivity of personal data in these contexts is not static, but highly dependent on the operational environment. Even data not traditionally considered sensitive, such as names, affiliations, or locations, can, in context, pose serious risks to individuals' safety and rights. The sensitivity of data in humanitarian contexts is therefore relational: it depends on who processes it, who might access it, and what consequences could arise. For example, the disclosure of names of individuals perceived to be affiliated with a particular group, or geolocation data revealing the whereabouts of displaced

90 See para. 6 of Resolution "Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection".

91 GDPR, Recital 51.

communities, could have serious consequences in conflict-affected or politically unstable areas. In such contexts, the misuse – or mere exposure – of personal data can lead to retaliation, discrimination, or persecution.

This also means that sensitivity must be assessed as a dynamic concept. Humanitarian environments are inherently fluid, and shifts in political control or security conditions can rapidly and dramatically change the risk profile of specific data types. A piece of information that appears relatively benign in one context may become highly sensitive in another, or in the same context may evolve over time. This fluidity underscores the need for a contextual application of data protection principles, where risk analysis is an ongoing process to ensure the protection of the rights, dignity, and integrity of affected persons.[92]

The data protection frameworks of humanitarian organisations, such as the ICRC's Rules and UNHCR's Policy, acknowledge this by emphasising risk-based, context-specific approaches. These frameworks emphasise data protection by design, purpose limitation, data minimisation, and continuous assessment of risks through tools such as DPIAs. In highly dynamic environments, DPIAs must account for contingency scenarios and evolving threats, and be regularly updated as contexts change. They also promote strong security safeguards, tailored to the level of risk associated with each type of data.[93]

Finally, this reality of humanitarian contexts also calls for specific protocols for data breach response. Although notifying affected individuals of data breaches is a crucial step in mitigating risks, in contexts where notification may itself be operationally difficult or risky, the feasibility and effectiveness of notification procedures must be considered. Here too, the data protection framework provides essential guidance for balancing individual rights with humanitarian realities, reinforcing the need for measures that evolve with the context they are meant to serve.

92 See, for instance, Katja Lindskov Jacobsen, "Biometric data flows and unintended consequences of counterterrorism," *International Review of the Red Cross* 103, no. 916–917 (2021): 619–652, https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916. See also, Irwin Loy, "Biometric data and the Taliban: What are the risks?," *The New Humanitarian*, 2 September 2021, https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban; Eileen Guo and Hikmat Noori, "This is the real story of the Afghan biometric databases abandoned to the Taliban," *MIT Technology Review*, 30 August 2021, https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/; and Human Rights Watch, *New Evidence that Biometric Data Systems Imperil Afghans*, 30 March 2022, https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.

93 This is also reflected in the varying approaches to the application of data protection principles and requirements across different processing situations and technologies, as suggested by Marelli ed., *Handbook on Data Protection*, Part II, 75–329.

Testing Assumptions

When analysing and applying data protection requirements in humanitarian contexts, these analyses are often based on a number of assumptions. As mentioned above, for example, it is commonly assumed that people in need of humanitarian assistance do not often have a genuine choice as to whether to accept the processing of their personal data, and that essential humanitarian services are, by definition, indispensable. In these circumstances, it is often assumed that individuals are not entirely free to choose, and that, therefore, consent cannot be used as a legal basis for processing data, as discussed below under *Beyond Consent: Ensuring Lawfulness and Fairness*. It is also sometimes assumed that, due to the complexity of the technologies used and the nature of the processing operations involved, it is difficult for people to fully understand the risks and benefits involved in the specific processing proposed. These assumptions are based on experience of working in humanitarian settings and are often supported by anecdotal evidence. But they are assumptions nonetheless, and they deserve critical examination.

As discussed earlier, the primary objective of data protection regulation is to ensure the respect of the rights and dignity of individuals when their personal data is processed, as well as to establish accountability of data controllers. In light of this, humanitarian organisations have over time been increasingly looking for ways to test these assumptions and to understand how affected persons live and experience the use of digital technologies and data – both in general and within the humanitarian sector specifically.

In response, humanitarian organisations have increasingly invested in initiatives that directly engage with affected populations to better understand their concerns, perspectives, and expectations. The objective of these workstreams is to use the concepts and requirements provided by data protection frameworks not just to ensure compliance, but also to achieve meaningful communication, strengthen transparency, and ensure that accountability mechanisms genuinely reflect the lived realities of those in crises.

Testing these assumptions requires recognising that experiences with technology and data handling in humanitarian settings are shaped by a variety of contextual factors, including local leadership structures, institutional trust, past experiences of surveillance or exploitation, and prevailing concerns about security.[94] Failing to account for these elements can lead even the best-intentioned data practices to inadvertently cause confusion, mistrust, or new vulnerabilities.[95]

94 For further discussion, see Chapter 17, "'Context matters': Studying Perceptions of Data Protection in Humanitarian Action".

95 Elysée Nouvet et al., "Opportunities, Limits and Challenges of Perception Studies for Humanitarian Contexts," *Canadian Journal of Development Studies / Revue Canadienne*

This has contributed to a broader, more nuanced understanding of data protection requirements: one that goes well beyond a purely legalistic approach and incorporates context-sensitive, community-driven perspectives. In this way, personal data protection has evolved not only as a lens for analysing the complex dynamics linked to the use of technology and data in humanitarian settings, but also as a valuable framework for the humanitarian sector to engage with affected populations in ways that put their dignity and agency at the centre.[96]

Impact on the Operating Modalities of Humanitarian Organisations

The second major impact of digital transformation on humanitarian action concerns the ability of organisations to maintain the modalities through which they operate in a neutral, independent, and trusted manner. As humanitarian work increasingly relies on complex digital infrastructure, often involving multiple third-party actors and transborder data flows, preserving the exclusively humanitarian character of data and systems has become more difficult. Even when access to data by third parties is lawful or incidental, it can undermine the conditions of trust and acceptance that humanitarian action depends on, and in some cases, jeopardise the safety of affected individuals.

In this environment, data protection plays a critical role, not only by offering technical safeguards, but by reinforcing the core principles that underpin humanitarian action. This section examines this issue, and how legal protections such as the privileges and immunities of IOs, combined with purpose limitation, serve as a barrier against third-party misuse and a foundation for trust. It also explores how these principles have been integrated and recognised in global discussions as part of the broader humanitarian diplomacy agenda, and then turns inward to consider the institutional capacities required to maintain cybersecurity and ensure operational resilience as part of this trust-building exercise, which are necessary to ensure responsible and effective humanitarian operations.

Together, these elements show how data protection not only helps manage risk, but also preserves the conditions under which humanitarian action remains possible, accepted, and trusted.

---

d'études du Développement 37, no. 3 (2 July 2016): 358–377, https://doi.org/10.1080/02255189.2015.1120659.

96 This contribution is described in detail in Chapter 20, "Data protection in the times of artificial intelligence: towards a digital humanism".

The Challenge of Third-Party Access and Surveillance and the Impact on Trust

In today's digital humanitarian landscape, trust is both essential and increasingly fragile. In crisis contexts, trust in humanitarian actors is the condition for persons affected by humanitarian emergencies to have access to essential humanitarian services. It enables humanitarian organisations to gain safe and sustained access to affected areas, and individuals to be willing to seek and receive humanitarian assistance. This trust is rooted in the understanding that humanitarian actors deliver services that are of a purely humanitarian nature, operate solely on the basis of humanitarian priorities, sustained by the principles of neutrality, impartiality, and independence, and that any information shared with them will be used exclusively for humanitarian purposes.[97]

For affected persons, trust is built, among other factors, on the promise by humanitarian organisations that the information they collect will be used for exclusively humanitarian purposes and will not be accessed and repurposed by third parties for ends that are incompatible with this promise. For parties to conflict or other stakeholders in situations of violence, trust rests on the understanding that humanitarian organisations operate in a neutral, impartial, and independent manner, and that whatever they witness, the data they collect, and the activities they carry out are exclusively humanitarian in nature and do not end up favouring one side over another.

This exclusively humanitarian "purpose specification" is, in the case of humanitarian organisations that are IOs, safeguarded by their privileges and immunities. These legal protections help prevent third parties from compelling access to data held by an IO without its agreement, and reinforce the principle that humanitarian information should not be diverted for political, security, or commercial ends. In doing so, they serve as a first line of defence, ensuring that data is used solely for its intended humanitarian purpose and thereby helping preserve the trust and neutrality on which humanitarian action depends.[98]

97 See, for instance, Red Cross Red Crescent Magazine, "Why Data Protection Is Critical to Humanitarian Action," January 2021, https://www.rcrcmagazine.org/2021/01/data-protection-critical-humanitarian-action/.

98 Resolution on Privacy and International Humanitarian Action by the International Conference of Privacy and Data Protection Commissioners, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf, explicitly highlights the risks associated with data transfers to humanitarian organisations that do not benefit from privileges and immunities, stating: "*Humanitarian organisations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally*".

However, as the digital footprint of humanitarian operations and the complexity of data flows with third parties expand, so do the risks of access to humanitarian data by third parties (through other third parties), and the repurposing of data.

Data initially collected for exclusively humanitarian purposes by a humanitarian organisation may, intentionally (e.g. through processing arrangements with third-party providers to deliver a programme) or inadvertently (e.g. whether due to hacking and other adverse cyber operations, or due to surveillance of the third-party processors), become available to non-humanitarian parties. These parties may repurpose this data for entirely different ends, such as commercial exploitation (corporate surveillance) or migration control or law enforcement (institutional surveillance).[99]

Even when such access is conducted under legitimate and lawful prerogatives (data gathered from non-IOs), it may still be incompatible with the exclusively humanitarian purpose for which the data was originally collected.[100] In some cases, it may lead to adverse impacts for the individuals in question,

99 The risk that authorities could pressure humanitarian organisations to share data for non-humanitarian purposes was notably highlighted in the above Resolution on Privacy and International Humanitarian Action, Explanatory Statement No. 5.

100 See para. 9 of "Joint Statement by the Group of Friends of the Protection of Civilians in Armed Conflicts," *Federal Department of Foreign Affairs (FDFA)*, 27 May 2020, https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/reden.html/content/missions/mission-new-york/en/meta/speeches/2020/may/27/joint-statement-by-the-group-of-friends-of-the-protection-of-civ, stating "*Digital technologies have helped protecting civilians in situations of armed conflicts and have offered a range of opportunities (...) At the same time, these technologies have also been misused thus exacerbating violence*". Paras. 10 and notably 11 of Resolution "Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection", urging "*States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement, (…) or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of RFL services*". Similarly, explanatory statement no. 5 of the Resolution on Privacy and International Humanitarian Action by the International Conference of Privacy and Data Protection Commissioners, states that "*Humanitarian organisations (…) may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally*". The Organization of American States (OAS), *Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection* urges OAS Member States to "*refrain from requesting Personal Data collected by humanitarian organisations, whenever the intent behind the request is to use the Data for non-humanitarian purposes, as this may have a serious impact on the beneficiaries of humanitarian services and be detrimental to their safety and to humanitarian action more generally*", 80. See also CCDCOE, *Scenario 25: Cyber Disruption of Humanitarian Assistance*, Cyber Law Toolkit, accessed 26 March 2025, https://cyberlaw.ccdcoe.org/wiki/Scenario_25:_Cyber_disruption_of_humanitarian_assistance, and Marelli, "Hacking Humanitarians".

including discrimination, repatriation, or retaliation against the data subjects. Such access and repurposing, therefore, risk fundamentally breaching the trust between humanitarian organisations and the people they aim to serve.

Ensuring the Recognition of Humanitarian Principles in the Digital Age

The principle of purpose limitation is, therefore, not only essential for ensuring trust with affected populations; it is also vital to safeguarding the neutrality, independence, and impartiality of humanitarian action in the face of growing digital interdependencies and third-party involvement, where data is frequently processed by commercial entities, transferred across borders, and subject to surveillance laws that may be incompatible with humanitarian principles. Ensuring that the humanitarian mandate is not undermined by the digital systems through which humanitarian services are now often delivered has thus become a priority of humanitarian diplomacy. As digital technologies reshape the way humanitarian organisations operate, significant efforts have been made to ensure that these core humanitarian principles, particularly the use of data for exclusively humanitarian purposes, are recognised, respected, and upheld in broader regulatory and policy environments.

Concrete steps have been taken to address this. As noted, the 2019 RFL Resolution explicitly calls for cooperation between States and humanitarian actors to ensure that personal data is not used in ways that compromise the humanitarian nature of the work or erode trust in humanitarian services.[101]

This recognition has since been reaffirmed and extended. The 2024 Movement Resolution on protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict (the ICT Resolution) reaffirms the RFL Resolution and emphasises that the issues addressed in that resolution are also important for the protection of other humanitarian data outside the realm of restoring family links.[102] The RFL Resolution was further supported by the Group of Friends, a coalition of 18 UN member and observer States formed to defend the principles of the UN Charter and promote multilateralism and

101 Para. 11 of Resolution "Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection": "*urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement, and in conformity with Article 2, including paragraph 5 thereof, of the Statutes of the Movement, or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of RFL services*".

102 "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict", Resolution (34th International Conference of the Red Cross Red Crescent Movement, October 2024): 2, https://rcrcconference.org/app/uploads/2024/10/34IC_R2-ICT-EN.pdf.

diplomacy,[103] in the context of a joint statement on the protection of civilians in armed conflict.[104]

The importance of humanitarian purpose limitation has also been recognised beyond the Movement. The 2019 GPA Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management underscores the need for safeguards tailored to the specific sensitivities of humanitarian data processing.[105] Similarly, the 2021 OAS Guidelines acknowledge the potential risks of repurposing humanitarian data, stating that Member States should refrain from seeking access to personal data collected by humanitarian organisations when this access could be incompatible with the exclusively humanitarian nature of their work, as this could seriously impact beneficiaries and jeopardise both their access to essential humanitarian services and humanitarian operations more broadly.[106]

These efforts are part of a growing recognition that humanitarian action must not be left out of the digital rulemaking processes that shape global standards. Ensuring that humanitarian principles, especially purpose limitation, are embedded in these frameworks is essential to preserving the trust and access on which humanitarian operations depend. Data protection, therefore, becomes not only a safeguard against harm but a lever for ensuring responsible humanitarian action in an increasingly complex digital ecosystem.

Institutional Resilience and Cybersecurity Readiness

The ability of humanitarian organisations to safeguard the exclusively humanitarian nature of their operations increasingly depends not only on more global recognition of their importance, but also on their own internal capacity to protect digital systems from misuse, intrusion, and repurposing. As the humanitarian sector becomes more reliant on digital technologies to deliver aid and protection, cybersecurity has become crucial to ensure neutrality and principled action.

103 "About Us", *Group of Friends in Defense of the Charter of the United Nations*, https://www.gof-uncharter.org/about-us.

104 FDFA, "Joint Statement by the Group of Friends of the Protection of Civilians on Cyber-Attacks Against Critical Infrastructure".

105 Explanatory statement of the International Conference of Privacy and Data Protection Commissioners, *Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management*, 42nd International Conference, 2020, https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-International-Aid-EN.pdf.

106 12th principle, "Exceptions," in OAS, *Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection.*

In this context, strong institutional cybersecurity capacities play a dual role. First, they help prevent unauthorised access to humanitarian systems, shielding sensitive information from surveillance, exploitation, and other cyber threats. Second, they reinforce organisations' abilities to uphold purpose limitation by ensuring that data entrusted to humanitarian actors is not diverted or compromised through external intrusion (including by virtue of data being processed through third-party processors). Without resilient digital infrastructure and clear protections against third-party access, even well-designed data protection policies risk being undermined in practice.

These risks are not hypothetical. Recent years have seen a marked increase in hostile cyber operations targeting humanitarian actors,[107] which can compromise their ability to provide protection and assistance to people affected by armed conflict.[108] At the same time, the increasing reliance on third-party digital service providers – often governed by different legal and regulatory frameworks – raises complex legal, technical, and operational questions, particularly regarding the security and confidentiality of sensitive data. These challenges make it imperative for humanitarian organisations to define their cyber-perimeters, develop a robust cybersecurity strategy, and establish clear legal and technical safeguards to uphold their independence, neutrality, and impartiality in the digital sphere.[109]

Looking at recent history, the ICRC's Delegation for Cyberspace and Global Cyber Hub, established in Luxembourg in 2022, embodies this commitment by providing a dedicated institutional space to support, protect, and deploy digital services to communities in a way that is neutral, impartial, and independent.[110] The Delegation not only facilitates operational resilience but also serves as a platform for developing new ways to ensure adherence to the fundamental principles in an evolving digital landscape.

Ultimately, preserving the independence, neutrality, and impartiality of humanitarian organisations in the digital age requires technical, diplomatic,

107 See, for instance, https://www.icrc.org/en/statement/cyber-operations-create-additional-risks-peoples-security-and-well-being.

108 The 2020 cyberattack on the RFL network, which potentially exposed the personal data of half a million vulnerable individuals, underscores how third-party dependencies can create critical vulnerabilities, leaving humanitarian organisations exposed to the same types of cyber threats that targeted major technology providers in incidents such as the SolarWinds hack. See, Massimo Marelli, "The SolarWinds hack: Lessons for international humanitarian organisations," *International Review of the Red Cross* 104, no. 919 (28 March 2022): 1267–1284, https://doi.org/10.1017/S1816383122000194. For further discussion, see also Chapter 12, "By the Book, Beyond and Backwards? Ethical considerations on the 2022 data breach affecting the Family Links Network of the Red Cross Red Crescent Movement".

109 For more on this, see Marelli, "Hacking Humanitarians," 367–387.

110 ICRC, "Luxembourg," https://www.icrc.org/en/where-we-work/luxembourg.

and institutional efforts. As digital threats evolve, institutional resilience and cybersecurity readiness are essential pillars of humanitarian trust and access. In this sense, data protection must be understood not only as a regulatory tool but as part of a broader digital architecture that enables principled humanitarian action.

Looking Ahead

As digital transformation continues to reshape humanitarian action, data protection frameworks have provided essential tools not only for mitigating risks but also for upholding the humanitarian principles on which trust and access depend. Yet, the pace of technological innovation shows no signs of slowing, and the humanitarian sector must continuously adapt. New digital tools, actors, and expectations will keep emerging, and geopolitics keep morphing, often faster than regulatory, operational, or ethical frameworks can evolve.

Responding to this challenge requires sustained foresight, collaboration, and investment. It means reflecting on past experiences and lessons learned, while also proactively preparing for the future. This section will explore how humanitarian actors can do so by maintaining mechanisms and cross-sector collaboration to monitor and make sense of technological trends, investing in research and development (R&D) to ensure that technologies are adapted to humanitarian realities and constraints, and addressing persistent challenges by strengthening internal capacity and building trusted partnerships with donors.

To ensure that humanitarian action remains principled, safe, and trusted in the digital age, the sector must go beyond reactive compliance. It must share knowledge and best practices, and shape the technologies it uses and the standards by which it operates to ensure digital transformation serves, rather than compromises, the rights, dignity, and safety of affected populations.

A Technology Observatory

One of the clearest lessons from the past ten years is the importance of cooperation with academia, civil society, and the tech industry to maintain a "technology observatory": a space to detect new technologies early, as they emerge, assess opportunities for deployment, and map their implications and challenges. Such observatories serve as early warning systems and incubators of responsible innovation, enabling the sector to prepare guidance for the safe and ethical use of new tools, shape policy responses, and direct R&D to ensure they are fit for humanitarian purpose.

A notable example of such collaboration is the ICRC's partnership with the Brussels Privacy Hub to convene the working series that eventually led to the publication of the Handbook on Data Protection in Humanitarian Action

in 2017. Now in its third edition, the Handbook remains an important reference, offering practical guidance on integrating data protection principles into humanitarian programming.[111]

Further advancing the responsible use of humanitarian data, the ICRC, in partnership with the OCHA Centre for Humanitarian Data and the Federal Department of Foreign Affairs of Switzerland, launched the Humanitarian Data and Trust Initiative (HDTI).[112] Its key objectives were to establish policy spaces to discuss priority themes linked to the digital transformation of the humanitarian sector, establish outreach initiatives to socialise these topics, and advance research to inform decision-making. Overall, there was an explicit intent to bring relatively niche topics to a broader audience to further raise awareness of the challenges and opportunities that were being created and explored within the humanitarian sector. The 2021 DigitHarium initiative, for example, was established to provide a collaborative space where practitioners from various fields could address the digital dilemmas impacting humanitarian action. During its run, the DigitHarium called on different experts each month to discuss a new trend or technology affecting humanitarian action, through online dialogues, debates, articles, and podcasts. These discussions focused on responsibly integrating digital solutions into humanitarian operations, minimising data collection to what is essential, and ensuring the protection of data subjects' rights.[113]

From the experience of bringing these topics to different audiences, the series of Symposia on Cybersecurity and Data Protection in Humanitarian Action, launched by the ICRC Delegation for Cyberspace in collaboration with the Ministry of Foreign and European Affairs (MFEA) of Luxembourg and other partners, was born. Each Symposium creates a space for experts from different sectors to tackle the intersection of cybersecurity, data protection, and humanitarian action through working groups and hackathons, promoting open and free discussions to address these critical issues.[114]

111 Marelli, *Handbook on Data Protection*.

112 "Humanitarian Data and Trust Initiative," *ICRC*, *OCHA*, *and FDFA*, https://centre.humdata.org/wp-content/uploads/2020/09/Humanitarian_Data_and_Trust_Initiative_HDTI_concept-09.2020.pdf.

113 "DigitHarium," *ICRC*, accessed 18 February 2025, https://www.icrc.org/en/digitharium.

114 Building on the success of the first edition in November 2022, the second edition of the Symposium took place from January 2024 in Luxembourg. It brought together almost 250 experts from more than 30 countries, representing humanitarian organisations, governments, cybersecurity agencies, data protection authorities, technology companies, civil society, and academia. For more information, see "At the Intersection of Humanitarian Action and Cyberspace," *ICRC*, 11 February 2025, accessed 18 February 2025, https://www.icrc.org/en/article/symposium-intersection-humanitarian-action-and-cyberspace. For the post-symposium report, see "Symposium: Cybersecurity and Data Protection in

Maintaining – and indeed strengthening – a capacity to convene relevant stakeholders to anticipate and detect emerging technologies, identify the opportunities, questions, concerns, and dilemmas they bring, and develop guidance as to how to best navigate them will remain crucial for the humanitarian sector in the years ahead, as new technologies, or new ways of using existing ones, come to the fore, and as financial constraints and rising humanitarian needs may increase the pressure to deploy them rapidly.

Research & Development: Advancing the State-of-the-Art

Despite concerted efforts to ensure comprehensive risk mapping, foster multi-stakeholder collaboration, and implement robust data protection frameworks, significant challenges persist, notably due to limitations in available technology.

Addressing these challenges requires proactive R&D to ensure that technological advancements align with humanitarian realities to ensure the safeguarding of the rights and dignity of affected individuals. In this sense, the use of biometrics for registration in humanitarian aid distribution is an interesting example. Biometric-based identification systems are often touted as a solution to issues of fraud, aid duplication, and transparency.[115] However, solutions available off-the-shelf are not designed to protect personal data against the specific threats and risks that occur in humanitarian contexts and conflict zones. Since the risks posed by biometrics stem from the very properties that make them appealing – uniqueness, universality, permanence – the application of data protection in the handling of biometric data of vulnerable people is paramount.

The ICRC Policy on the Processing of Biometric Data[116] underscores the need to remain at the forefront of technological innovation to continuously evaluate whether biometric data processing poses risks to the rights or safety of data subjects. To better respond to these challenges, collaborations with experts in different fields are fundamental. In continuation of its long-standing partnership with the *École Polytechnique Fédérale de Lausanne* (EPFL), the ICRC supported research into a safe digital aid-distribution system addressing those challenges and keeping biometrics as a potential solution. This resulted in a privacy-by-design end-to-end decentralised design based on

Humanitarian Action," *ICRC*, https://shop.icrc.org/symposium-cybersecurity-and-data-protection-in-humanitarian-action-pdf-en.html.

115 For further discussion, see Chapter 4, "The Logic of Biometrics and Organisational Accountability".

116 The Policy on the Processing of Biometric Data outlines both technical and legal safeguards to ensure that sensitive biometrics data is handled with integrity and respects the rights and dignity of individuals. See *Policy on the Processing of Biometric Data by the ICRC*.

the use of tokens that could integrate the use of biometric data in humanitarian programmes without exposing individuals to undue risks.[117]

The ICRC partnered with non-profit technology company Simprints and the Idiap Research Institute in Switzerland to develop a privacy-preserving biometric identification system. The idea was to leverage existing academic research in the domain of biometric template protection and implement an algorithm that can demonstrate the irreversibility, renewability, and unlinkability of biometric templates.[118]

The ICRC has also piloted privacy-preserving biometric verification within its RedSafe platform, a secure digital environment for beneficiaries. This proof of concept demonstrated the feasibility of integrating biometric protections that enhance security without compromising individual privacy.[119]

As such, by investing in responsible R&D and embedding data protection by design,[120] the ICRC seeks to ensure that technological advancements serve humanitarian needs without compromising privacy or security. As emerging technologies continue to reshape the sector, a proactive and ethical approach to innovation remains essential to safeguarding the rights and dignity of affected populations. This may involve taking humanitarian organisations out of their traditional space of action and into R&D partnerships to ensure that the technology that is used is the one that is needed and the one that is fit for purpose.

117 Boya Wang et al., "Not yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution," in *2023 IEEE Symposium on Security and Privacy (SP)* (IEEE, 2023): 645–663, https://arxiv.org/abs/2303.17343. See also Chapter 4, "The logic of biometrics and organisational accountability".

118 More specifically, the collaboration resulted in a working prototype of an end-to-end biometric identification system integrating a privacy-preserving biometric template protection algorithm. The algorithm ensures that stored biometric templates cannot be reversed to reconstruct raw biometric data, mitigating risks in case of data breaches. It also allows users to generate new biometric templates if their data is compromised and prevents cross-matching between databases, ensuring unlinkability across different applications. For more information on the algorithm used to protect biometric templates in this solution, see: Vedrana Krivokuća Hahn and Sébastien Marcel, "Towards Protecting Face Embeddings in Mobile Face Verification Scenarios," 27 January 2022, https://doi.org/10.1109/TBIOM.2022.3140472. For the open-source code, see: "Simprints/Biometrics-SimPolyProtect," Kotlin (2024; repr., Simprints, 21 January 2025), https://github.com/Simprints/Biometrics-SimPolyProtect.

119 For further discussion, see Chapter 3, "The challenges of building RedSafe, a secure digital humanitarian platform. An unsafe journey?".

120 The notion of data protection by design in humanitarian settings, its specific objectives, modalities, and methodologies, are elaborated in detail in Carmela Troncoso and Wouter Lueks, "Designing for Data Protection in Humanitarian Action," *Handbook on Data Protection in Humanitarian Action*, 3rd ed., chapter. 6.

Capacity-Building and Stakeholder Responsibility

As humanitarian organisations continue to navigate a fast-changing digital landscape, new challenges are emerging that test the resilience of existing data protection efforts. Ensuring responsible digital transformation will depend not only on anticipating technological developments but also on reinforcing the institutional foundations that make data protection effective in practice. This includes investing in capacity-building to equip staff with the skills and awareness necessary for responsible data handling, and fostering a shared understanding across the sector to enable coordination and trust.

First off, to meet these emerging challenges, capacity-building efforts must evolve in both scope and strategy. Responsible digital transformation requires a fundamental institutional and cultural shift toward embedding data protection and ethical considerations into the operationalisation of humanitarian efforts. Strengthening knowledge and awareness at all levels of an organisation is critical to ensuring that data protection is understood and implemented effectively, not merely as a compliance requirement, but as a cornerstone of trust in humanitarian action.

In addition, as highlighted so far, the primary concern in this space is that of ensuring the respect of the rights and dignity of people affected by humanitarian emergencies. This requires the entire humanitarian sector to be effectively implementing data protection requirements. The existence of a common baseline in the handling of personal data is also an important element at the basis of trust between humanitarian organisations, which can facilitate cooperation and, where necessary, responsible data sharing.

To that end, the ICRC has over the years developed a range of training programmes, both internal and external, to ensure that humanitarian staff are equipped with the knowledge and skills necessary to handle personal data responsibly. Collaboration with institutions such as Maastricht University,[121]

121 The Data Protection Officer (DPO) Humanitarian Action Certification is a specialised training programme developed by the European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Faculty of Law, and the ICRC DPO, in collaboration with OCHA, IOM, IFRC, and UNHCR, to equip humanitarian DPOs with the necessary expertise to navigate the complexities of data protection in humanitarian action, particularly in the face of evolving technologies, regulatory challenges, and ethical considerations. See "ECPC-HA Humanitarian Aid Certified DPO," *Maastricht University*, https://www.maastrichtuniversity.nl/research/ecpc/professional-certification-education/ecpc-ha-humanitarian-aid-certified-dpo.

EPFL,[122] and the Federal Institute of Technology Zurich (ETH Zürich),[123] has been key in building capacity and a deeper understanding of responsible use of technology among humanitarian professionals. Ensuring that relevant and up-to-date training opportunities are available to the staff of humanitarian organisations at all levels will remain a key priority area. Well-designed training fosters a shared understanding across and within organisations, strengthens accountability, and helps reassure affected populations that their data will be handled responsibly.[124]

Finally, capacity-building must extend to engagement with donors, whose data use expectations have a growing influence on how humanitarian data is collected, shared, and governed.[125] While transparency is vital, donor requirements should not undermine humanitarian principles or create new risks for affected populations. Ongoing dialogue and principled data-sharing agreements are essential to ensuring that digital transformation is not only effective but also ethically grounded and protective of the people it aims to serve.[126]

Conclusion

The digital transformation of humanitarian action has reshaped the sector in fundamental ways. Far from being driven by technological hype alone, this shift reflects a deeper imperative: to meet rising humanitarian needs with limited resources, to respond effectively to increasingly complex crises, and to uphold transparency and accountability to both affected communities and donors.

122 For instance, the Humanitarian Action in the Digital Age MOOC, launched by EPFL, the ICRC, and Médecins Sans Frontières (MSF), provides humanitarian professionals with a comprehensive understanding of Information and Communication Technologies (ICT), helping them navigate risks, opportunities, and ethical considerations in digital humanitarian work. See "MOOC: Humanitarian Action in the Digital Age," *EPFL*, 13 July 2023, https://actu.epfl.ch/news/mooc-humanitarian-action-in-the-digital-age/.

123 Data protection being closely related to cybersecurity, the ICRC developed, in cooperation with the ETHZ Centre for Security Studies, a specialised course on the policy and geopolitics of cybersecurity. See "Educational Programs," *Engineering for Humanitarian Action (EHA)*, https://eha.swiss/educational-programmes/.

124 For further discussion, see Chapter 19, "Teaching Data Protection as Trust-Building".

125 See, for instance, Vincent Cassard, Stuart Campo, and Jonas Belina, "Responsible data sharing between humanitarian organisations and donors: towards a common approach," *Humanitarian Law & Policy Blog* (blog), 22 June 2023, https://blogs.icrc.org/law-and-policy/2023/06/22/responsible-data-sharing-humanitarian-organizations-common-approach/.

126 For further discussion, see Chapter 15, "Data sharing between humanitarian organisations and donors: accountability, transparency, and data protection in principled humanitarian action".

While digital tools have enabled faster, broader, and more data-informed responses, they have also introduced new risks. Expanding digital footprints, fragmented data ecosystems, and growing reliance on third-party infrastructure have made it more difficult to safeguard the rights, dignity, and agency of affected individuals, and to maintain the trusted, neutral, and independent character of humanitarian operations.

At the heart of this transformation lies data. How data is collected, governed, and used shapes not only the delivery of aid and protection, but also individual outcomes and the trust on which humanitarian access and acceptance depend.

In this evolving landscape, data protection has become an essential pillar of responsible humanitarian action. Rooted in a rights-based approach, it offers not only legal safeguards but also a practical, value-driven framework to address digital risks, clarify roles and responsibilities across a complex network of actors, and translate humanitarian principles into digital practice.

This section has explored two major impacts of the new digital landscape. First, it has become significantly harder to uphold the rights and dignity of affected populations, particularly in contexts where individuals are often disempowered, dependent on aid and protection, and have limited ability to meaningfully influence how their data is used. Second, the operating modalities of humanitarian organisations have come under strain, as data passes through a web of third-party providers and regulatory regimes, making it more difficult to preserve the exclusively humanitarian character of operations and the trust on which they rely.

In both cases, data protection has emerged as a critical enabler. As a rights-based approach, it places the individual and their dignity at the centre. By helping the sector understand and navigate complex data flows, reinforcing transparency and accountability mechanisms, and enabling a context-sensitive approach to digital operations, it helps restore an essential degree of agency and control to affected populations, which is the foundation of human dignity. At the same time, it strengthens operational safeguards and serves as a lever for humanitarian diplomacy to ensure the recognition of purpose limitation and other fundamental principles at a global level, thereby preserving the conditions under which humanitarian action remains possible, accepted, and trusted.

Looking ahead, ensuring that the sector's digital transformation remains responsible and fit for purpose will require continued investment in research, cross-sector collaboration, innovation, and capacity-building. This includes maintaining observatories to anticipate emerging trends and develop responsible technologies, equipping humanitarian actors with the tools and knowledge they need, and fostering trust-based relationships with donors that uphold data protection standards and ethical use.

The themes explored in this section – humanitarian operations, technological transformation, local perspectives, cross-border governance, diplomacy, and responsible innovation – are deeply interconnected. The challenges and solutions in one area influence and shape developments in another. It is precisely this intersection of issues that makes it essential to bring together diverse perspectives – academic analyses, policy reflections, and personal insights from practitioners – in a compound edited volume. By reflecting on the evolution of data protection in humanitarian action over the past decade and the lessons learned, while anticipating the challenges and opportunities that lie ahead, this work aims to foster a shared commitment to safeguarding the rights and dignity of those humanitarian action seeks to serve, ensuring that it can continue to evolve responsibly in the digital age.

PART 2

Humanitarian Action in the Digital Age

PART 2.1

An Evolving Humanitarian Space

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

2

FROM DISCONNECTED TO CONNECTED

How Ten Years of Increasing Connectivity for Crisis-Affected Communities Has Increased the Importance of Personal Data Protection

Betty (Jia Li) Wang and John Warnes

Introduction

Protecting personal data is vital to upholding the safety, dignity, and rights of affected populations, a responsibility that is increasingly acknowledged and embedded within legal frameworks across many jurisdictions.[1] In the digital age, this protection has become more critical than ever,[2] encompassing efforts to ensure the integrity, confidentiality, and availability of personal data, while safeguarding the rights, freedoms, and dignity of those whose information is collected and processed. The approach to achieve such outcomes is often realised through a broad range of measures, such as data security, data minimisation, risk assessments, and accountability frameworks outlining data sharing parameters with third parties.

Over the last decade, connectivity levels have increased rapidly[3] and more crisis-affected communities have gained access to the internet.[4] In parallel,

1 International Committee of the Red Cross (ICRC), The ICRC data protection framework, https://www.icrc.org/en/document/icrc-data-protection-framework.

2 Massimo Marelli, "Introduction," ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition, Massimo Marelli ed. (Cambridge, 2024), https://doi.org/10.1017/9781009414630.

3 GSMA, *The State of Mobile Internet Connectivity Report 2024*, Figure 1, 2024, 10, https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf; GSMA, *The Digital Worlds of Displacement-Affected Communities*, 2023, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/the-digital-worlds-of-displacement-affected-communities/

4 GSMA, *The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in the Way*, 2019, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/the-digital-lives-of-refugees/.

DOI: 10.4324/9781003650164-5

data protection considerations in humanitarian action have evolved as a practice over the same period globally – the focus of this book.

In this chapter, we look back at the dynamics in the humanitarian sector around connectivity and the emergence of connectivity as aid solutions, which have become increasingly common practice. Connectivity *as* aid refers to the provision of internet access, mobile networks, and digital communication tools as a form of humanitarian assistance and differs from connectivity *for* aid, which focuses on providing connectivity to support humanitarian responders in carrying out their work.[5] We will explore how the rapid expansion of connectivity amongst crisis-affected populations has created complex new challenges relating to data protection in humanitarian action. We will focus specifically on how increased connectivity as aid requires a data protection lens and the connectivity considerations that data protection practitioners need to take into account.

Background and Trends

Increased Availability and Access to Connectivity

The digital age has elevated the importance and complexity of data protection in humanitarian settings.

Over the past decade, global availability and access to connectivity have surged. In 2023, approximately 68% of the world's population was online; however, this figure dropped significantly to just 35% in less developed countries.[6] Mobile internet penetration has increased from 33% to 57% globally over the past ten years,[7] with users in some settings having access to 4G and even 5G networks.[8] Nonetheless, penetration rates differ greatly by region as less than 30% of the Sub-Saharan African population is connected to mobile internet.[9] Despite persisting disparities in access, mobile phones have become

5 Aaron Martin and John Warnes, "Connectivity as Aid," ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition, Massimo Marelli ed. (Cambridge, 2024): 274–287, https://doi.org/10.1017/9781009414630.021. For a longer discussion on the distinction and its implications, see: ICRC, "DigitHarium Month #5: Providing (and Denying) Connectivity during Crises," 9 July 2021, https://www.icrc.org/en/digitharium/digitharium-month-5.

6 International Telecommunication Union (ITU), "Measuring digital development: Facts and Figures 2024," accessed 10 May 2025, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

7 GSMA, *The State of Mobile Internet Connectivity Report 2024*.

8 GSMA, *The State of Mobile Internet Connectivity Report 2024*.

9 GSMA, *The State of Mobile Internet Connectivity Report 2024*.

increasingly affordable and widespread, with roughly 73% of the global population aged ten and older owning a mobile device in 2022.[10]

This growth in digital access and usage has not occurred in isolation but has been shaped by a dynamic ecosystem of technological innovation, supported by cross-sector investments and partnerships.

Expansion in terrestrial network infrastructure, including fibre and cellular, has significantly accelerated the global digital transformation in the past decade. Amongst many, governments from Rwanda[11] to Indonesia[12] have launched digital acceleration projects, often with support from development institutions and the private sector aimed at broadband and digital public service expansion with a focus on last-mile connectivity. Major technology firms have also contributed to global connectivity infrastructure. These companies are taking significant stakes in undersea cable capacity, including one initiative deploying 50,000 km of cable to connect five continents.[13] In parallel, innovations in mobile network technologies such as 4G/5G technology and small-scale base stations[14] have demonstrated the potential to provide more flexible and rapid deployment of connectivity in emergency contexts, facilitating real-time communication, situational awareness, and early warning systems in humanitarian contexts.[15]

Technological advances in non-terrestrial networks are also playing a more critical role in bridging connectivity gaps in remote and crisis-affected regions. This includes satellite solutions that extend the reach of terrestrial communication networks to last-mile areas. While these technologies have existed for decades, recent innovations such as low Earth orbit (LEO) satellite constellations have ignited renewed enthusiasm, particularly within the humanitarian sector.[16] Companies, in many cases owned by the world's major technology

10 ITU, "Mobile Phone Ownership," 24 November 2022, https://www.itu.int/itu-d/reports/statistics/2022/11/24/ff22-mobile-phone-ownership/.

11 Rwanda Information Society Authority (RISA), "Rwanda Digital Acceleration Project," accessed 10 May 2025, https://www.risa.gov.rw/projects/rdap.

12 ASEAN Briefing, "Indonesia's Palapa Ring: Bringing Connectivity to the Archipelago," 5 October 2023, https://www.aseanbriefing.com/news/indonesias-palapa-ring-bringing-connectivity-archipelago/.

13 Liv McMahon, "Meta plans globe-spanning sub-sea internet cable," *BBC News*, 17 April 2024, https://www.bbc.com/news/articles/ckgrgz8271go.

14 Nicol Turner Lee, "Enabling Opportunities: 5G, the Internet of Things, and Communities of Color," *Brookings*, 30 January 2020, https://www.brookings.edu/articles/enabling-opportunities-5g-the-internet-of-things-and-communities-of-color/.

15 Jamie Alexander Greig, "Wireless Mesh Networks as Community Hubs: Analysis of Small-Scale Wireless Mesh Networks and Community-Centered Technology Training Open Access," *Journal of Information Policy* (2018) Volume 8: 232–266, https://doi.org/10.5325/jinfopoli.8.2018.0232.

16 GSMA, *The Humanitarian Mobile Coverage Gap*, May 2024, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads

companies as much as by incumbent satellite players, have launched LEO constellations capable of delivering high-speed, low-latency broadband in areas where traditional infrastructure is unfeasible.[17] These systems can offer rapid connectivity deployment to facilitate access and service delivery in humanitarian emergencies.

Finally, community-driven initiatives[18] such as community networks have gained prominence, especially in marginalised and low-resource settings. Supported by low-cost wireless technologies and participatory governance models, these locally managed systems offer a sustainable alternative to top-down connectivity approaches.

Growing Connectivity Access for Affected Populations

In this global environment of enhanced connectivity, populations affected by crises are increasingly online and expect to access information, resources, assistance, and services through digital channels.[19] In parallel, humanitarian practitioners are increasingly aware of the considerable value displaced populations place on connectivity. The 2015 Mediterranean crisis catalysed a shift in perception for many, whereby the internet was acknowledged not only as an essential tool for aid workers, but as a vital component of aid for affected populations themselves.[20] Reports from this time illustrate the indispensability of smartphones, as forcibly displaced populations used them for navigation, communication, and accessing vital information and services.[21] Similarly in other geographies, refugees are reported to sacrifice a significant portion

/2024/05/ConnectivityInCrises2_R_Web-1.pdf.

17 Claudia Marquina, "How low-earth orbit satellite technology can connect the unconnected," *World Economic Forum*, 18 February 2022, https://www.weforum.org/stories/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/.

18 UNHCR Innovation Service, *Community-led Connectivity, UNHCR Innovation Service*, May 2020, https://www.unhcr.org/innovation/wp-content/uploads/2020/05/Community-led-Connectivity-WEB052020.pdf.

19 GSMA, *The Digital Worlds of Displacement-Affected Communities;* GSMA, *The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in the Way.*

20 Rakesh Bharania and Mark Silverman, "Protective by design: safely delivering connectivity as aid," *Humanitarian Law & Policy*, ICRC, 8 July 2021, https://blogs.icrc.org/law-and-policy/2021/07/08/protective-by-design-connectivity-as-aid/.

21 Alessandra Ram, "Smartphones Bring Solace and Aid to Desperate Refugees," *WIRED*, 5 December 2015, https://www.wired.com/2015/12/smartphone-syrian-refugee-crisis/; Patrick Witty, "See How Smartphones Have Become a Lifeline for Refugees," *TIME*, 8 October 2015, https://time.com/4062120/see-how-smartphones-have-become-a-lifeline-for-refugees/; Lin Taylor, "Internet in Greek Migrant Camps as Important as Food, Water: Aid Groups," *Reuters*, 22 July 2016, https://www.reuters.com/article/us-europe-migrants-greece-internet/internet-in-greek-migrant-camps-as-important-as-food-water-aid-groups-idUSKCN102209/.

of their food rations or income to buy data.[22] More recently, the COVID-19 pandemic dramatically accelerated the digitalisation of aid delivery to sustain humanitarian service delivery, given restrictions on in-person engagement.[23] This theme is further elaborated in Section 2.2: Understanding the Digital Transformation of the Humanitarian Space Through Data Protection.

Connectivity as Aid Interventions as a Response

While information and communication technology (ICT) has long been foundational to humanitarian interventions, the growing demand for connectivity and digital services in recent years among crisis-affected populations has increased the public recognition that connectivity is a basic right[24] as it is essential to accessing lifesaving information, education, health, feedback channels for humanitarian assistance, and more. This trend has catalysed the implementation of connectivity as aid solutions as a central pillar of response efforts. Initially, many connectivity as aid interventions effectively extended connectivity for aid solutions out to a wider target population that included crisis-affected communities. Over time, approaches have been evolving towards facilitation, with humanitarian organisations working directly with a wider network of stakeholders to enable commercial connectivity services to be accessed by communities. This has involved predominantly, but not exclusively, mobile network operators as well as governments, which create the regulatory regimes that facilitate inclusion and ultimately provide a national framework for universal access.[25]

Since the 2015 Mediterranean crisis, building on traditional connectivity for aid approaches, humanitarian actors have piloted connectivity as aid solutions involving internet access points in camps and informal settlements.[26]

22 UNHCR Innovation Service, *Connectivity for Everyone*, accessed 10 May 2025, https://www.unhcr.org/innovation/connectivity-for-everyone/.

23 John Bryant et al., *Bridging Humanitarian Digital Divides During COVID-19*, Humanitarian Policy Group, November 2020, https://media.odi.org/documents/Bridging_humanitarian_digital_divides_during_Covid-19.pdf.

24 World Food Programme (WFP), *Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2023 to implement the outcomes of the WSIS*, Commission on Science and Technology for Development (CSTD), 2024, https://unctad.org/system/files/non-official-document/wsis2023_c31_wfp_en.pdf.

25 For a longer discussion on the distinction and its implications, see: ICRC, "DigitHarium Month #5: Providing (and Denying) Connectivity during Crises," *ICRC*, 9 July 2021. https://www.icrc.org/en/digitharium/digitharium-month-5.

26 Madeline Kane, "For Refugees, Internet Is a Lifeline," *NetHope*, 17 May 2016, https://nethope.org/articles/for-refugees-internet-is-a-lifeline/; ANSA, "Refugee Info Bus Offers Migrants Internet, Legal Assistance," *InfoMigrants*, 25 September 2017, https://www.infomigrants.net/en/post/5240/refugee-info-bus-offers-migrants-internet-legal-assistance;

The COVID-19 pandemic further underscored the importance of digital service delivery in humanitarian response.[27] From the onset of the pandemic, humanitarian, government, and private sector actors implemented different contactless processes, from remote digital identity verification systems[28] to digital cash assistance via mobile money.[29] Communication via digital channels also increased significantly as displaced communities could receive critical updates about the pandemic and services available from humanitarian actors through SMS and commercial services such as WhatsApp.[30] In the wake of the pandemic, various sectors continue to innovate and digitalise their services to reach affected populations more efficiently and effectively, such as by expanding digital learning offerings[31] and accelerating efforts to connect schools and young people to the internet.[32]

Finally, the multi-stakeholder "Connectivity for Refugees" initiative, founded by the UN High Commissioner for Refugees (UNHCR), the International Telecommunication Union (ITU), the Global System for Mobile Communications Association (GSMA), and the Government of Luxembourg, which was launched in 2023, seeks to build much more expansive connectivity delivery approaches in forced displacement settings, aiming to advance connectivity for over 20 million forcibly displaced and stateless people by 2030.[33] These efforts are very much grounded in the aforemen-

---

Helen Nianias, "Homemade Wi-Fi routers are giving refugee camps a lifeline," *WIRED*, 22 October 2018, https://www.wired.com/story/refugee-wifi-project-jangala-worldwide-tribe/.

27 GSMA, *COVID-19 and digital humanitarian action: Trends, risks and the path forward*, 2021, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/gsma_resources/covid-19-and-digital-humanitarian-action/.

28 UNHCR, "Registration and Profiling," accessed 10 May 2025, https://reporting.unhcr.org/registration-and-profiling-194.

29 UNHCR, *UNHCR CASH ASSISTANCE AND COVID – 19*, accessed 10 May 2025, https://www.unhcr.org/sites/default/files/legacy-pdf/5eb55d427.pdf; WFP, *WFP and COVID-19*, accessed 10 May 2025, https://cdn.wfp.org/2020/covid19-response/.

30 GSMA, *The Digital Worlds of Displacement-Affected Communities*; UNHCR Innovation Service, "Taking Innovation Global with Two-Way Communications with Refugees," *Medium*, 27 February 2025, https://medium.com/unhcr-innovation-service/taking-innovation-global-with-two-way-communications-with-refugees-8b4d51adef0b.

31 Vodafone Foundation, "Instant Network Schools," accessed 10 May 2025, https://www.vodafone.com/vodafone-foundation/focus-areas/instant-network-schools; UNESCO, "UNESCO's Global Education Coalition," accessed 10 May 2025, https://www.unesco.org/en/global-education-coalition; UNHCR, "Refugee Connected Education Challenge," UNHCR UK, accessed 10 May 2025, https://www.unhcr.org/uk/what-we-do/build-better-futures/education/refugee-connected-education-challenge.

32 UNICEF, "Giga: Connecting Every School to the Internet," UNICEF Innovation, accessed 10 May 2025, https://www.unicef.org/innovation/giga.

33 Connectivity for Refugees, "Connectivity for Refugees," accessed 10 May 2025, https://www.refugeeconnectivity.org.

tioned partnership dynamics that move away from traditional connectivity for aid approaches towards market-oriented sustainable solutions.

Consistent Barriers to Connectivity Access

While connectivity as aid approaches have become increasingly popular, many displaced communities continue to face significant and disproportionate barriers in accessing even the most basic connectivity services. Despite the widely recognised benefits of mobile network coverage, available data indicates that people affected by crises are disproportionately situated in areas without such coverage.[34]

This exclusion exacerbates existing vulnerabilities, and the risks of crises have become increasingly severe in the digital age when they occur in areas without mobile network coverage. First, individuals may be unable to raise concerns or request help in times of danger, undermining both personal safety and community resilience.[35] Connectivity is critical for enabling two-way communication between humanitarians and crisis-affected communities. Second, gaps in internet access hinder the effective delivery of humanitarian assistance.[36] As aid becomes increasingly digitalised, lack of connectivity can delay or even exclude individuals from receiving necessary services. Finally, without reliable access to the internet, displaced individuals face reduced economic opportunities, reinforcing dependency on aid and limiting pathways towards self-reliance and resilience.[37]

Increasingly Complex Data Protection Challenges

Many facets of connectivity as aid are relevant to data protection. While core elements of this delivery area focus on data security – for instance, combating the hacking of networking equipment or the exploitation of software vulnerabilities, there are additional dimensions fitting a wider scope of data protection where connectivity impacts fundamental rights, such as users' data rights, and create legal obligations for data controllers. Key risks include data being

34 GSMA, *The State of Mobile Internet Connectivity Report 2024*; Filippo Grandi, "Internet and Mobile Connectivity for Refugees – Leaving No One Behind," UNHCR Innovation Service, accessed 10 May 2025, https://www.unhcr.org/innovation/internet-mobile-connectivity-refugees-leaving-no-one-behind/.

35 GSMA, *Connectivity in Crisis: The Humanitarian Implications of Connectivity for Crisis-Affected Communities*, Mobile for Development, January 2024, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/01/Connectivity-in-Crises_Web_Singles.pdf.

36 GSMA, *Connectivity in Crisis*.

37 UNHCR, *Connecting Refugees*, September 2016, https://www.unhcr.org/media/connecting-refugees.

utilised by controllers for purposes beyond purpose specification, the opacity of data flows, lack of appropriate data protection impact assessments (DPIAs), or "do no harm" analysis when deploying connectivity as aid solutions, and a lack of adequate user engagement, thus impacting agency, accountability, and the overall dignity of users of connectivity as aid services.

Overall, developments in connectivity as aid present a somewhat mixed landscape when it comes to data protection in humanitarian action, with dichotomies that need to be carefully navigated by practitioners. For crisis-affected communities, the use of connectivity services has certainly grown, yet in many parts of the world, many are still left behind. Enhanced connectivity has resulted in greater digital transformation in the humanitarian sector; however, connectivity as aid is still far from being a predictable and mainstreamed component of a humanitarian response. The approaches have evolved too, with a notable increase in complex multi-stakeholder partnerships to advance connectivity and digital adoption, moving away from more straightforward delivery models. Yet the latter are often relied upon substantially, in particular in more remote locations.

As the focus of this book is on data protection, the central message is as follows: there have been increased quantities of personal data shared and processed due to the increased uptake of digital channels,[38] underpinned by connectivity as aid interventions, and the trend is set to continue. While these interventions aim to enhance access and inclusion for affected populations, they also introduce significant data protection risks, such as opaque data flows between systems, unclear accountability among multiple delivery actors, and potential data misuse by third parties, all of which are further explored in the next part of this chapter.[39] Ultimately, the link between connectivity as aid interventions and data protection risks is clear and increasingly complex. This dynamic warrants not only the analysis in this chapter, but also demands awareness and action from actors involved in delivering aid to affected populations, including humanitarian and data protection practitioners.

While this cannot fully cover all aspects of this evolving landscape, it will be sufficient to provide some insights into what connectivity as aid and data protection practitioners need to address, particularly pertaining to data security, in their immediate futures and in their approaches over the next ten years of data protection in humanitarian action and thereafter, including the benefits of greater collaboration with each other.

38 Martin and Warnes, "Connectivity as Aid," *Handbook on Data Protection*.
39 Martin and Warnes, "Connectivity as Aid," *Handbook on Data Protection*.

The Growing Role of Connectivity in the Humanitarian Context Has Exacerbated the Complexities of Data Protection Risks and Mitigations for Vulnerable Populations

Connectivity as Aid Vulnerabilities for Affected Populations

As noted, there has been significant growth in connectivity as aid interventions and therefore also a more connected crisis-affected population. However, these people should not be viewed as typical "consumers" of ICT services; rather, they are often uniquely and significantly vulnerable to data protection threats due to their status.

The nature of user vulnerability is rarely something elaborated on within national regulatory regimes for telecommunications. Most relevant frameworks, ranging from telecommunications access and universal service to data protection policies, make little reference to the unique protection needs of crisis-affected populations. In some cases, regimes may be ineffective at challenging invasions of privacy coming from other jurisdictions.[40] For example, local laws requiring third-party disclosure of metadata could allow government entities to readily identify individuals and specific communities (e.g. women, LGBTQ+).

Beyond the regulatory environment, individual users' digital, data, and media literacy and knowledge can also influence their ability to understand the context in which they are operating and critically assess considerations around safe connections and secure digital practice.[41] Depending on the jurisdiction and the access users have been granted to apps on their devices, affected populations may find governments or other actors seeking to intervene in or conduct surveillance on individuals' devices or connections, whether consensual or not, to understand their digital footprint.[42] An individual's history of

40 ICRC and Privacy International, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, ICRC, October 2018, https://reliefweb.int/report/world/humanitarian-metadata-problem-doing-no-harm-digital-era-october-2018#:~:text=The%20report%20%E2%80%93%20The%20humanitarian%20metadata,travel%20routines%20or%20frequent%20contacts.

41 UNHCR, *Connecting with Confidence: Managing Digital Risks to Refugee Connectivity*, March 2021, https://www.unhcr.org/innovation/wp-content/uploads/2021/03/CWC-Managing-Digital-Risks-To-Refugee-Connectivity-Report.pdf.

42 Morgan Meaker, "Europe is using smartphone data as a weapon to deport refugees," *WIRED*, 2 July 2018, https://www.wired.com/story/europe-immigration-refugees-smartphone-metadata-deportations/; Office of the High Commissioner for Human Rights (OHCHR), "Digital technologies at borders: A threat to people on the move," 9 October 2023, https://www.ohchr.org/en/stories/2023/10/digital-technologies-borders-threat-people-move; Joel Brown, "Digital Cages: How ICE Uses Digital Surveillance to Track Migrants," *The Brink*, 26 January 2024, https://www.bu.edu/articles/2024/digital-cages-surveillance-to-track-migrants/.

connectivity is under the microscope, and aware of this, users' behaviour will undoubtedly change.

Finally, we come to connectivity services themselves. The fact of being a largely liberalised sector globally, with the private sector delivering a service which is noted by actors such as the Emergency Telecommunications Cluster (ETC) as being a "basic right",[43] has resulted in a variety of partnership approaches that warrant scrutiny not only from a data protection perspective, but in relation to humanitarian principles. As noted, the complex layers delivering connectivity as aid solutions at scale often require multiple third parties to be involved, a dynamic that may not be immediately visible to non-experts. Private service provision through a complex web of actors may limit not only the ability of humanitarian organisations but also governments to guarantee such a right.

Changing Geopolitics of Telecommunications

As noted earlier, LEO satellite solutions are increasingly offering unprecedented connectivity capabilities in crisis settings at lower cost.[44] For crisis-affected communities, the geopolitics of telecommunications may have far-reaching impacts on not only the safeguarding of individuals' personal data but also wider protection concerns, especially in proximity to conflict.

In the current competitive and polarised environment, the decision to use a particular technological tool is likely to be increasingly perceived as a political choice. Relationships between governments and telecommunications players are increasingly intertwined. In this context, choosing a technology provider may come with unique legal and political considerations often attached to the interests of both company shareholders and of the government of the country in which the company is headquartered.[45] States and private actors are also accelerating the race to control digital technologies and increase their commercial and political influence at the global level.[46] Governments have been quick to exert what influence they can on these shifting telecommunications

43 WFP, *Submissions from entities in the United Nations system, international organizations and other stakeholders on their efforts in 2023 to implement the outcomes of the WSIS*.

44 Lam Le, "China's SpaceSail Is Expanding Where Elon Musk Is Stumbling," *Rest of World*, 31 March 2025, https://restofworld.org/2025/chinas-spacesail-is-expanding-where-elon-musk-is-stumbling/.

45 Kieran Smith and Peggy Hollinger, "Top Donald Trump official tells Europe to choose between US or Chinese communications tech," *Financial Times*, 15 April 2025, https://www.ft.com/content/0a086fc2-1955-4ded-8558-6f9f85a0679d.

46 "The Battle for Digital Supremacy," *The Economist*, 15 March 2018, https://www.economist.com/leaders/2018/03/15/the-battle-for-digital-supremacy; World Economic Forum, "Fourth Industrial Revolution," accessed 10 May 2025, https://www.weforum.org/focus/fourth-industrial-revolution/.

dynamics through regulation, from withholding approval for certain satellite technologies despite their widespread humanitarian use[47] to introducing economic incentives for the adoption of one solution over another.[48] While this dynamic is not new, the stakes are increasing, as is the impact on the humanitarian sector and its ability to safeguard the sensitive data of vulnerable populations in the face of governments which could wield influence over companies based in their jurisdiction.

With such tensions in play, many have exerted, or sought to exert, influence on humanitarian organisations exploring connectivity solutions. Connectivity as aid practitioners in the past may have focused on the technical; however, there is now an increasing impetus to examine all risk factors, including the political dimensions, which can influence the protection of personal data through these networks.[49] In such situations, humanitarian actors may lose their ability to choose privacy-preserving or ethically appropriate tools that prioritise the protection of affected populations. By exposing personal data to systems or actors that may neglect human rights, this approach undermines the core humanitarian commitment to "do no harm".

Technologies of Both Civilian and Military Use

The adoption of telecommunications for both civilian and military use is often referred to as "dual-use" technology.[50] The ability of such technology to service both humanitarian needs and military operations by parties to conflicts or entities associated with them is another emerging dilemma for connectivity as aid practitioners. The nature of this technology could compromise the neutrality of humanitarian actors and expose affected populations to surveillance, manipulation, and targeting, including the restriction or shutdown of connectivity services. The recent shifts in satellite technology, with the expansion of LEO services, give the issue a new and heightened significance as covered by media outlets in ongoing conflicts.[51] This raises challenges for

47 William Wroblewski, "Tired of spotty internet, Bolivians are smuggling in Starlink," *Rest of World*, 13 February 2025, https://restofworld.org/2025/bolivians-smuggle-starlink-to-escape-china-backed-internet/.

48 Adonijah Nedge, "Kenya proposes tenfold fee hike for satellite ISPs like Starlink," *TechCabal*, 8 January 2025, https://techcabal.com/2025/01/08/kenya-starlink-higher-fees/.

49 Aaron Martin and Quito Tsui, "Humanitarian Connectivity in Crisis," *Global Policy Journal*, 2 June 2025, https://www.globalpolicyjournal.com/blog/02/06/2025/humanitarian-connectivity-crisis.

50 University of Cambridge, *Dual-Use Goods, Technology and Software*, Import Export Hub, accessed 26 May 2025, https://www.importexport.admin.cam.ac.uk/controlled-items/dual-use-goods-technology-and-software.

51 Matthew Fitzgerald and Cort Thompson, "What Does Starlink's Participation in Ukrainian Defense Reveal About U.S. Space Policy?" *Lawfare*, 26 April 2022, https://

the opportunity and ethics of building communication systems that rely more and more exclusively on military-adjacent systems to transfer affected individuals' data and conflict-sensitive information, a concern shared by the United Nations Office for Outer Space Affairs (UNOOSA)[52] and the International Committee of the Red Cross (ICRC).[53]

Dual-use technology can be vulnerable to the interests of certain customers within a technology company's portfolio. For example, if a government were to be contracting commercial LEO services for military purposes used in a conflict where it was also providing humanitarian assistance in the form of connectivity as aid, organisations and communities alike may become concerned about whether the use of such civilian telecommunications services might be perceived as making them an active party to conflict.[54]

Private-Sector Involvement

Delivering connectivity as aid solutions often requires the involvement of multiple third parties, including private technology companies that may introduce added data protection risks for vulnerable populations.

The objectives of private technology companies often diverge from humanitarian imperatives. Many of these firms operate on models centred on data monetisation or surveillance-based advertising – practices that can directly conflict with humanitarian commitments to do no harm, ensure data minimisation, and uphold affected populations' dignity and rights. The collaboration between humanitarian organisations and technology companies often lacks transparency and frequently operates without clear disclosure of data handling practices, leaving affected individuals unaware of how their personal information is collected, stored, and used. This reality is further emphasised by Access Now's private tech mapping exercise, where it found no "instance of

---

www.lawfaremedia.org/article/what-does-starlinks-participation-ukrainian-defense-reveal-about-us-space-policy; James Fitzgerald, "Ukraine war: Elon Musk's SpaceX firm bars Kyiv from using Starlink tech for drone control," *BBC News*, 9 February 2023, https://www.bbc.com/news/world-europe-64579267; Emily de La Bruyère and Nathan Picarsic, "The Perils of Allowing Elon Musk's Starlink Into Gaza," *Foundation for Defense of Democracies*, 14 November 2023, https://www.fdd.org/analysis/2023/11/14/the-perils-of-allowing-elon-musks-starlink-into-gaza/.

52 United Nations Office for Outer Space Affairs. "Benefits of Space: International Peace and Security," accessed 10 May 2025, https://www.unoosa.org/oosa/en/benefits-of-space/international-peace-and-security.html.

53 Svenja Berrang, "How Would IHL Apply to Hostilities in Outer Space?" *ICRC*, 2 November 2023, https://blogs.icrc.org/law-and-policy/2023/11/02/how-would-ihl-apply-to-hostilities-in-outer-space/.

54 Kubo Mač ák and Mauro Vignati, "Civilianization of Digital Operations: A Risky Trend," *Lawfare*, 5 April 2023, https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend.

public adherence of a tech company to humanitarian principles, explanation of their protection-based approach in digital development, nor public disclosure of the impact of their humanitarian intervention beyond a PR release".[55]

This opacity in data handling can lead to violations of data protection and privacy principles,[56] as individuals in crisis situations may be unable to provide informed consent or exercise control over their data, particularly when there may be no other alternatives as essential assistance is only available digitally. Furthermore, the consolidation of data management in the hands of a few large tech firms increases the risk of data misuse, especially when these companies have business models centred on data monetisation or surveillance-based advertising. Telecom providers have been known to share customers' location data without consent or to fail to take adequate steps to safeguard data.[57] For humanitarian contexts, the risks are even more pronounced as the misuse of location data or other personal information can lead to threats to safety, exposure to persecution, and loss of access to services. In response, humanitarian actors should proactively assess technology partners' policies on data handling and implement strict contractual safeguards to prevent secondary use, data commodification, or misuse, particularly in contexts where affected individuals have little recourse against or understanding of such risks.

Data Protection Barriers to Connecting with Confidence

While individuals do face data protection risks due to the geopolitics and shifts in the telecommunications industry, everyday usage threats (e.g. phone security and online scams) are more frequent and can be more severe. Below we examine data security risks specifically, as an important element of broader data protection concerns, linked to connectivity from the perspective of community members based on the operational experiences of the authors.

In the context of connectivity as aid, it is important to highlight the implications of different connectivity models and the overall user experience. Firstly, where a user has an individual service contract likely with a mobile network operator (MNO) for their own personal use (or potentially that of their family), and, secondly, on a communal level where a connection is shared amongst users and is often provided by a third party, who in turn has a contract with a

55 Giulio Coppi, *Mapping Humanitarian Tech: Exposing Protection Gaps in Digital Transformation Programmes*, Access Now, February 2024, https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf.

56 United Nations System Chief Executives Board for Coordination, *Principles on Personal Data Protection and Privacy*, accessed 10 May 2025, https://unsceb.org/privacy-principles.

57 David Shepardson, "FCC fines US wireless carriers over illegal location data sharing," *Reuters*, 29 April 2024, https://www.reuters.com/business/media-telecom/fcc-fines-us-wireless-carriers-nearly-200-million-over-illegal-location-data-2024-04-29/.

service provider. While, historically, connectivity as aid has focused on communal provision first and foremost, trends outlined earlier point to individual access becoming a more significant and predominant form of connectivity in humanitarian situations.

Individual Access

SIM registration can be a key challenge in humanitarian settings, especially in forced displacement contexts.[58] Registration often requires users to provide personal information (e.g. name, national identification, and date of birth). A user's IMSI (unique SIM number) and IMEI (unique device number) are logged by service providers to facilitate billing, along with the time and location of transactions (e.g. calls and messages), and information associated with SIM card registration.[59] Furthermore, Call Detail Records[60] can be used to identify population movements as well as to model demographic and economic profiles of individuals. When combined, this data available to service providers can enable them to identify, monitor, and target communities.

Where humanitarian organisations are involved in facilitating connectivity provision from an MNO, their role would likely be limited to dialogue and sharing of key information, such as the location of crisis-affected communities requiring service. MNOs can often have complex ownership structures,[61] which can influence a crisis-affected community's trust in a provider. In some contexts, anecdotal evidence points to trust being maintained where an MNO was providing consistent service and was trusted prior to, during, and after a crisis or flight. Conversely, and particularly in situations of flight, displaced populations may be concerned about government authorities from their country of origin having access to data that is transferred across the different operating companies of an MNO. As such, humanitarian organisations are exploring wider concepts of due diligence grounded in human rights that may

58 UNHCR Innovation Service, "Displaced and Disconnected," accessed 10 May 2025, https://www.unhcr.org/innovation/displaced-and-disconnected/.

59 Caitlin N. Howarth et al., "Establishing Mobile Connectivity in Refugees Camps," Mercy Corps and Harvard Humanitarian Initiative, August 2020, https://www.mercycorps.org/sites/default/files/2021-03/04-MIC-WiFi-Guide-FINAL.pdf.

60 Data logs created by phone exchanges or telecommunications equipment that document the details of telecommunications transactions, including phone calls, text messages, or data usage.

61 Vodafone, "Change in Vodafone's ownership of Vodacom Group and Vodacom Group's ownership of its South African subsidiary," *Vodafone News*, 11 June 2018, https://www.vodafone.com/news/empowering-people/vodacom-ownership; McKinsey & Company, "Reshaping Telco Organizations to Meet the Industry's New Challenges," McKinsey & Company, accessed 10 May 2025, https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/Telecoms/PDFs/Reshaping_telco_organizations.aspx.

provide a better approach, or bespoke frameworks, that capture the partnership dynamics with providers and better articulate the shared value in these collaborations.[62]

Depending on the perceived levels of trust of a particular brand or company, the user's digital literacy levels, and overall level of concern about their data security, individuals may be compelled to activate certain security features. Some refugees use virtual private networks (VPNs) to avoid monitoring or to circumvent local restrictions on certain websites or social media platforms.[63] In the 2021 UNHCR report, "Connecting with Confidence",[64] an analysis of users and uptake of VPNs demonstrated that a significant number of users were opting to use free VPN services that were often compromised (both intentionally by a fraudulent provider or unintentionally due to compromised software) with malware.

Device security issues are also a challenge for individual users. In many humanitarian contexts, affected populations have cheaper, more affordable models or older devices[65] and therefore may lack the most recent security updates and patches, which leave their devices vulnerable to exploitation.[66] Certain community members are also reliant on higher speed connections provided by humanitarians in the community to update security features.[67] Device safety is further complicated in environments where device sharing or lending is commonplace; not all users follow security practices (e.g. signing out of a user account), which can enhance digital risks.

Communal Level Access

While there are many permutations of communal level access, simply connecting to an open Wi-Fi network established at a refugee camp may be sufficient to attract the attention of actors interested in the identity, location, activity, and movement of whoever holds the connected mobile device.

From Wi-Fi hotspots to connected community centres and cyber cafes, community facilities managed by humanitarian organisations provide

62 United Nations High Commissioner for Refugees (UNHCR), "Human Rights Due Diligence," UNHCR Information Integrity Toolkit, 20 December 2024, https://www.unhcr.org/handbooks/informationintegrity/practical-tools/human-rights-due-diligence.

63 Adrienne Yandell, "'All refugees have smartphones…' and here's what we can do about it," *Medium*, 26 July 2016, https://medium.com/@ayandell/all-refugees-have-smartphones-and-heres-what-we-can-do-about-it-511b5bf848b0.

64 UNHCR, *Connecting with Confidence*.

65 Howarth et al., "Establishing Mobile Connectivity in Refugee Camps".

66 UNHCR, *Connecting with Confidence*.

67 UNHCR, *Connecting with Confidence*.

connectivity services and, sometimes, devices to individuals.[68] Given that such centres' governance frameworks are generally adopted *ad hoc*, many lack adequate measures in terms of network security, cybersecurity, and information security.

In this model, complexities arise as providers are also responsible for the connectivity service itself. With the rise of more comparatively affordable LEO satellite connections, there has been an uptick in local entrepreneurs serving as connectivity resellers either formally or informally.[69] This is a relatively significant development, as the responsibility for the connection rests with a community member who may or may not be exercising due care and caution with regard to network security, or be acting in a reputable manner regarding traffic flowing over the network. It may be possible for them to track, target, and follow an individual based on their usage of the local area network.[70] Metadata attached to browsing habits as well as device information may also be vulnerable. A lack of capabilities on the part of that individual or organisation may also result in poor cybersecurity practices at the network level, potentially exposing users to risk due to, for instance, a lack of firewalls. In many cases, users are also required by providers to give personal data to access communal networks as part of the promotion of the inclusion of marginalised groups. This data may increase data protection risks when cross-referenced with other datasets.

Physical spaces can significantly impact user data practices, especially in overcrowded service centres where users may unintentionally expose sensitive information such as passwords. Additionally, unsecured hard copy records, such as sign-in books requesting personal details, further heighten data risks. Communal devices pose risks such as users forgetting to log out or saving sensitive files locally, making them vulnerable to misuse. They can also be exploited through tools like keyloggers that capture keystrokes or monitor activity.

Poor user habits and limited digital literacy at communal facilities also pose significant risks to personal data security. Language barriers, low technical skills, and inadequate understanding of digital safety may make it difficult for refugees to detect scams or manage data consent.[71] Without strong govern-

68 Giulia Balestra, "When innovation is yet another Connected Community Centre: Connectivity at the margins of innovation," *Medium*, 17 May 2019, https://medium.com/unhcr-innovation-service/when-innovation-is-yet-another-connected-community-centre-connectivity-at-the-margins-6bcb4227fc54.

69 Kakuma Ventures, accessed on 12 May 2025, https://kakumaventures.com/.

70 Brent Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society* 3, no. 2 (December 2016): 1–21, https://doi.org/10.1177/2053951716679679.

71 Khorshed Alam and Sophia Imran, "The Digital Divide and Social Inclusion among Refugee Migrants: A Case in Regional Australia," *Information Technology & People* 28, no. 2 (2015): 344–365, https://doi.org/10.1108/ITP-04-2014-0083.

ance frameworks on cybersecurity and data literacy components, these vulnerabilities are further amplified.

Emerging Connectivity Risks

The trends and dynamics outlined earlier have contributed to an evolving data protection risk landscape that is more complex than in the past. Users are sharing their data and allowing network and connectivity providers to generate data about them, though perhaps not willingly, in order to get connected through individual or community channels. As we move forward from a retrospective of the last ten years, we anticipate in the next decade that large-scale geopolitical questions will loom over modern connectivity service provision; however, the actual impact on end-users from a data protection risk standpoint remains to be seen.

The primary risks faced by users include fraud and scams, and the likelihood of such occurrences has strong links to the misuse of personal data and user behaviour. Other risks may include user exposure to profiling by non-humanitarian third parties, surveillance by malicious actors, monitoring (in some cases repression) linked with prevailing conflict and violence dynamics, and overall misuse by third parties for purposes incompatible with the exclusively humanitarian use expected from engagement with humanitarian actors. Building on the 'Connectivity as aid' chapter in the ICRC's Data Protection Handbook,[72] we now explore considerations and actions that can be taken by humanitarian practitioners engaged on these issues.

Implications for Data Protection Practitioners in the Humanitarian Context

The embrace of this digital transformation and connectivity programming must be accompanied by robust considerations and processes around data protection. Encouragingly, awareness and accountability around data protection risks are gaining traction amongst connectivity as aid practitioners, with leading humanitarian organisations beginning to take meaningful action, such as publishing and applying guidelines and reports about responsible use of technology and data in humanitarian contexts.[73] Yet, safeguarding against these risks cannot be achieved by humanitarian actors alone and requires the involvement of various stakeholders, including governments, affected communities, and private sector providers alike. Building collective responsibility

72 Martin and Warnes, "Connectivity as Aid," *Handbook on Data Protection*.
73 Bharania and Silverman, "Protective by design"; ICRC, *Handbook on Data Protection*.

across this ecosystem is critical to ensuring humanitarian principles are upheld in the digital age.

Humanitarian actors providing or facilitating connectivity as aid interventions must meaningfully integrate core humanitarian principles such as humanity, impartiality, neutrality, and independence into their project design and implementation, and in particular into how they integrate partnerships into delivery. Importantly, data collected or generated for humanitarian purposes should be used exclusively for such purposes, as articulated by the Group of Friends at the United Nations Security Council[74] and in accordance with the Organization of American States (OAS) Guidelines,[75] which emphasise the protection and purpose limitation of humanitarian data. In addition, integrating data protection thinking into connectivity as aid is still far from the norm and requires strengthening. Operationalising data protection principles requires robust, up-to-date assessments and frameworks to proactively manage evolving risks, even in the constrained timelines of rapid humanitarian response which can limit room for thorough and meaningful due diligence. DPIAs should be embedded in programme design to reflect shifting sociopolitical contexts, data access modalities, protection risks, and impacts on the neutrality, impartiality, and independence of humanitarian programmes. Given the growing prevalence of private sector involvement in connectivity deployment, rights-informed ethics and risk analyses should be standard in partnership frameworks to understand a partner's data practices and address any misalignment between humanitarian values and commercial imperatives. Organisations can also benefit from adopting a culture of continuous learning, adapting protections as technologies and threats evolve.[76]

For data protection practitioners, the trends around connectivity and the complex risk landscapes that are emerging may require, if not an update to tools such as DPIAs, at least guidance on how to carry them out, ensuring projects that process personal data consider the local connectivity context, looking at challenges emerging for users from the point of connection. This would include not only connectivity service provision by the humanitarian

74 Swiss representative to the UN, *Joint Statement by the Group of Friends of the Protection of Civilians on Cyber-Attacks Against Critical Infrastructure*, Swiss Confederation, 26 August 2020, https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-organizations/un/swiss-speeches-statements.html/content/missions/mission-new-york/en/meta/speeches/2020/august/26/joint-statement-by-the-group-of-friends-of-the-protection-of-civ.

75 Organization of American States (OAS), *Annual Report of the Inter-American Juridical Committee to the General Assembly*, 2021. https://www.oas.org/en/sla/iajc/docs/INFOANUAL.CJI.2021.ENG.pdf.

76 ICRC, "Q&A: Humanitarian operations, the spread of harmful information and data protection," 103, no. 916 (2021), https://international-review.icrc.org/articles/humanitarian-operations-harmful-information-data-protection-913#footnoteref15_4fhpx50.

organisation in question, but also local access dynamics with private sector actors (in line with the aforementioned individual and communal approaches) as well as user behaviour dynamics.

Beyond assessments and tools, new ways of working are vital. Digital protection must extend beyond headquarters and back-office systems to frontline operations.[77] Data protection officers and field staff, especially those deploying connectivity, can align more closely on connectivity solution design and data risk mitigation. Field-level information security should be strengthened given that digital vulnerabilities are often most acute at the local level. Integration of external stakeholders such as civil society, digital rights groups, or ethically-aligned tech firms in planning and deployment can further bolster the effectiveness and scale of data protection measures.[78] For example, in-country civil society organisations focused on digital protection issues could help deliver digital risk training to local communities with support from humanitarian organisations or other connectivity actors. Meanwhile, governments can consider leveraging the reach of local MNOs to extend public awareness campaigns.[79]

Finally, ensuring data protection thinking is integrated into emerging standards and norms around connectivity as aid is essential to ensure that programmes are protective by design. Minimum technical specifications for humanitarian connectivity should embed security and protection from the outset and adapt to evolving threats.[80] The ETC, for example, is exploring how to develop common approaches and standards for connectivity as aid solutions amongst a range of humanitarian and private sector partners.[81] The contents of such frameworks should speak to all actors (i.e. humanitarian actors and private firms) to ensure collective responsibility to uphold humanitarian principles, even if the roles differ from the stakeholder type to the context.

Beyond measures undertaken by humanitarian actors, active involvement and input from affected communities are required throughout a programme lifecycle to ensure data protection measures are contextual and effective. For example, anecdotal evidence suggests that geopolitical complexities with selecting certain connectivity solutions are best sense-checked with

77 Bharania and Silverman, "Protective by design".
78 ICRC, "Q&A: Humanitarian operations".
79 UNHCR, *Connecting with Confidence*.
80 Bharania and Silverman, "Protective by design".
81 Emergency Telecommunications Cluster (ETC), "Connectivity as Aid Consultations Wrapped up Last Week with Great Engagement from across the Sector," LinkedIn, December 2024, https://www.linkedin.com/posts/emergency-telecommunications-cluster_connectivity-as-aid-consultations-wrapped-up-activity-7267280694039506944-5TDa/; ETC, *ETC Plenary Meeting Minutes*, April 2025, https://www.etcluster.org/sites/default/files/documents/ETC%20Plenary%20meeting%20minutes_April%202025.pdf.

communities' perceptions, preferences, and concerns. Humanitarian actors can support this by empowering individuals to make informed decisions about digital participation and potential usage risks, providing accessible explanations of why technologies are being or should be used, how data is handled, and what consequences may arise.[82] Connectivity and data sharing must also remain a genuine choice. While many demand better access, others seek the right to opt out, arguing that such tools can reinforce inequality and external control.[83] Respecting this perspective is critical to maintaining impartiality and autonomy in digital humanitarian action.

Robust advocacy and capacity-building on data protection measures targeted at government authorities are essential, especially for agencies newly involved in crisis response which must be equipped to address the unique vulnerabilities and connectivity-related risks faced by affected populations, as well as ensuring the inclusion of data protection concerns for vulnerable populations within national digital strategies.[84] Close engagement with a diverse range of government bodies, including regulators, policymakers, and local security officials, can improve awareness of both offline and online threats and their impacts brought about by enhanced connectivity. In the context of humanitarian programmes, this could involve surveillance and cyber threats specific to crisis-affected populations.

At the same time, collaboration with private sector partners must be principled and deliberate. Whether acting as vendors or active contributors to humanitarian efforts, technology firms must adhere to conflict-sensitive practices, align with sector-specific standards, and uphold humanitarian ethics. Sustained dialogue between humanitarian actors and private companies can ensure that digital connectivity solutions are not only effective, but also preserve the dignity, safety, and rights of those they aim to serve through connectivity solutions.

Conclusion

In summary, the humanitarian sector has embraced digital transformation in the past decades, but with that comes a greater level of responsibility for humanitarian practitioners to protect personal data conduits of affected populations. In these settings, connectivity as aid is no longer optional, but essential, and must be implemented with safeguards that uphold data protection

82 ICRC, "Q&A: Humanitarian operations".

83 Lee Rainie and Janna Anderson, "Theme 4: More people will be connected and more will withdraw or refuse to participate," Pew Research Center, 6 June 2017, https://www.pewresearch.org/internet/2017/06/06/theme-4-more-people-will-be-connected-and-more-will-withdraw-or-refuse-to-participate/.

84 UNHCR, *Connecting with Confidence*.

and humanitarian principles. The growing risks posed by complex technologies, geopolitical entanglements, and cross-sector partnerships require new models of collaboration, regulation, and due diligence between humanitarian actors, governments, the private sector, and communities. As we move forward into the next decade, data protection must be seen not as an afterthought, and connectivity as aid not as peripheral, but both as central elements of the humanitarian response in the digital age.

3

THE CHALLENGES OF BUILDING REDSAFE, A SECURE DIGITAL HUMANITARIAN PLATFORM

An Unsafe Journey?

Romain Bircher[1]

Introduction

In May 2021, in Southern Africa, the International Committee of the Red Cross (ICRC) launched its first version of RedSafe,[2] the digital humanitarian platform. This marked the first attempt by the ICRC to deliver and test new digital services with a global, secure, independent, and privacy-by-design platform for people affected by conflicts and other humanitarian crises.

In April 2025, we launched the tenth version of RedSafe and it has been successfully piloted in Southern Africa and Central America.

RedSafe is a public platform and app managed by the ICRC but open to partners. It has been downloaded in these two pilot regions by more than 1,000,000 people. RedSafe provides a vault hosted by the ICRC, where people can save a copy of their personal documents and contacts, a map where people can locate themselves and find humanitarian services nearby. It provides alerts, self-protection tips, and trusted information on services delivered by the ICRC and 50 other humanitarian agencies, as well as including an

1 The opinions and views expressed in this article are the author's own as he offers a personal account based on his experience in leading the design of RedSafe. The opinions and views do not represent those of the International Committee of the Red Cross (ICRC). The author is grateful to the Challenge Team members for their endurance, skill and passion in co-creating RedSafe, namely to Marton Galanthay, Clara Palau Montava, Berta Panes, Vincent Graf Narbel, Michael Carcamo, Federico Siefinsider, Gil Talon, and Eduardo Ubierna Beguin. He is also grateful to all the people who believed in the idea and supported its implementation against all odds, starting with Charlotte Lindsey Curtet, our first sponsor, and Massimo Marelli, Head of the ICRC Data Protection Office.

2 See the RedSafe landing page at: https://www.icrc.org/en/redsafe.

DOI: 10.4324/9781003650164-6

offline mode and a feedback mechanism. RedSafe also serves as the main digital entry point for people to securely contact the ICRC and access its services. To preserve a good level of independence and legal protection, RedSafe is based on open-source technologies and its data is hosted on ICRC servers.

This is a personal account of the origins of the idea and vision behind this digital platform and the challenges we faced during this five-year journey, from the ideation phase to the end of the first pilot runs in 2024, to build and test a digital humanitarian platform.

This chapter focuses on the details of two specific challenges: the design of beneficiary-centric digital services and the creation of secure, privacy-by-design, and independent foundations.

Needs and Context

The ICRC operates in hostile contexts where violence, abuse, deception, misinformation, surveillance, forced displacement, family separation, and privation of essential services are widespread. People affected by conflicts and other crises need to do whatever they can to protect themselves and survive. This includes remaining in contact with relatives and people who can help them and accessing essential services and trusted information, while being careful not to expose themselves and their loved ones.

The range of services delivered by the ICRC is wide, as is the range of contexts in which it operates. These services are delivered directly or with partners, starting with the world's largest humanitarian network of staff and volunteers provided by the Red Cross and Red Crescent Movement.

The contexts in which the ICRC operates vary from full-fledged wars to protracted conflicts that can last for decades. Crises have regional and global humanitarian consequences, as they force people to flee their homes and impact people located elsewhere who are anxious for news of missing relatives.

The ICRC's action is guided by operational principles, with the most important ones summarised in the acronym NIIHA, i.e. neutral, impartial, independent humanitarian action.

The ICRC has seen the tremendous impact of communication technologies for good and for bad, with their trove of big data transmitted, traded, and exploited to provide value to individuals, benefits to companies, means of surveillance for security agencies, and strategic advantage for parties to conflicts.

To remain relevant, the ICRC has felt the need to invest both in new digital services and in understanding the impact of digital disruption on warfare, on people affected by humanitarian crises, and on the organisation itself. Facing a stream of changes, risks and opportunities, a shift in influence and power, we defined a strategy to onboard new digital technologies and adjust our approach, while preserving our values and principles. The "Information Environment Strategy", adopted in 2018, identified, among

other requirements to be fit for the future, the building and testing of a new secure and trusted digital platform, which we later called RedSafe.

We did not want to wait to be disrupted by new technologies. We felt the need to understand that shift and to invest in digital services, based upon field experience, peoples' needs, and our principles.

Building a platform for a global organisation is a complex and risky endeavour. When we speak about such platforms, we refer to hugely popular platforms, such as Amazon and Booking.com. We celebrate or criticise their impact but tend to disregard the challenges they faced and the many other failed attempts by competitors.

Building such a platform for the ICRC and its partners added extra challenges to the classical challenges any organisation faces with such an undertaking, due to the specific nature of the organisation, its context, and mandate. The development and deployment of RedSafe took five years. It was an exciting but unsafe journey, in the sense that we left our comfort zone to explore the unknown, deliver new digital services, and therefore learn by doing something we had never done before. Security, privacy, beneficiary-centric engagement, trust, and the do no harm principle had to be at the very heart of this endeavour.

The Origins

The idea of building RedSafe, an independent and beneficiary-centric digital platform, was rooted in humanitarian action. It emerged from two different experiences: the ICRC's interactions with leading tech companies in the early 2010s, and a series of field interviews, which started at the end of 2018, with people affected by humanitarian crises and with first responders.

Digital Disruption

One of those starting points was the result of my prior engagement in the early 2010s in leading the development of a new ecosystem of digital tools to support the ICRC's protection activities. While most of these tools were case management systems, we also decided to launch a new public version of our family links website.

The family links website[3] was first created to help people find missing relatives during the conflict in Kosovo at the end of the 1990s. It was used in other crises but did not evolve until the 2010s. Under certain circumstances, the ICRC could publish the names of people who were missing, pictures of people who were looking for missing relatives, or even let survivors self-publish

3 See the current version of the ICRC family links website: https://familylinks.icrc.org.

their names. Then on 12 January 2010 came the Haiti earthquake, which caused death and destruction on an unprecedented scale. We rapidly launched our family links website only to find out that all the names published there were republished, without prior agreement, on Google Person Finder, a new site launched by the tech giant… to do good. People who contacted us in the aftermath of the earthquake for their names to be deleted or to update the information on their whereabouts on the ICRC family links website could not easily obtain such deletions and changes on this Google website. Nor could we when we raised our concerns with the managers of Google Person Finder. Then discussions started, for the first time, with the tech giant to see whether we could collaborate and build a more ethical web model together or at least avoid creating confusion and harming people who need help in future humanitarian crises.

Years later, Facebook launched its own product, Facebook Safety Check, which enabled people, following a disaster, to notify their Facebook friends of their whereabouts.

Discussions with Google and Facebook did not lead to any partnership agreement, as their interests and the way they dealt with people's personal data clashed with the ICRC's way of doing things, which was in line with the emergence of a new and stronger data protection framework and our own data protection rules. But this dialogue was not in vain.

It helped us better understand these companies and raise their awareness of the negative impact of the uncontrolled publication of personal data in situations of political violence. As a concrete example, managers of Google Person Finder, following our advice, made the decision not to launch in countries impacted by protests during the Arab Spring. It also forced the ICRC to find new ways to engage with big tech companies on the impact of technologies in humanitarian crises.

We also understood that humanitarian and independent action could be disrupted at any time by big tech companies. It was time to invest, do it our way, and learn from it.

The Beneficiary Discovery Journey

Another starting point was a short mission we organised in December 2018 to Kenya, which launched a year-long series of field studies and interviews of potential beneficiaries and key stakeholders.

In Kakuma refugee camp, in northern Kenya, while I was interviewing a man who told me he had lost everything when he had to flee East Congo, the phone in his pocket was vibrating every ten seconds with notifications. He was concerned that communications he had via messaging apps with the friends he had left behind could reveal their allegiances and endanger them.

In contrast, in another part of the camp, a young boy, accompanied by his sister, was whispering to us about the torment of their flight from their village in Sudan, which was attacked by a militia and burned to the ground. To save their own lives, escape rape and slavery, they had to leave their parents, whom they presumed to be dead, behind, and walk hundreds of kilometres through one of the most dangerous areas on earth. The boy had a limb amputated following a snake bite. I saw that they were sharing a very basic feature phone, but I did not feel it appropriate to ask questions about its use. We ended our interview and referred them to Kenyan Red Cross volunteers who could help them trace their parents or confirm their deaths. The children did not know they could be helped to find out what happened to their relatives.

In another case, a Congolese asylum seeker we interviewed in Nairobi showed us a bundle of papers protected by a plastic sheet and taped to his chest under his shirt. He showed us a copy of his ID, police records, and a letter from the UN High Commissioner for Refugees. He did this with a trembling hand as he feared that somebody might steal or destroy them, or that they might fall into the hands of people who would identify him as a target. This bunch of crumpled papers and phone contacts was all he had. They gave him hope that one day, in Kenya or elsewhere, he could start a new life.

This experience in Kenya was the start of a long series of field missions and interviews with people who had fled zones of conflict or poverty, as well as with humanitarian staff and the authorities.

Among others, we interviewed Zimbabweans in a holding facility in South Africa waiting to be expelled, and we also met with people in the rural community of Zaka in Zimbabwe, close to the Mozambican border, where connectivity was limited.

We interviewed Venezuelans, who had been walking for weeks and had often been beaten and robbed, families with young children on the road from the border, crossing the Andes with only crocs and light clothing in the freezing cold of Berlin, in Colombia. We interviewed a father whose stillborn child had been disposed of as waste, as he and his wife did not have the means to pay for the burial.

In Honduras and Mexico, we interviewed Cubans using all types of messaging and entertainment apps, but also indigenous men from Guatemala who barely spoke Spanish sharing one phone and using only WhatsApp. In Coatzacoalcos, we interviewed a mother travelling with her six-month-old child and a young female cousin, waiting by the side of the railroad tracks to run and jump into the freight train, known as *La Bestia*, which would not stop, and to throw her baby to her cousin who would jump in first. We decided not to interview another woman also sitting by the railroad, surrounded by men, who first smiled when we approached her, and then suddenly cried out of fear and sadness.

We interviewed a girl who said that her own ID had no value, but the contact details on her phone of someone abroad could attract envy and put her in danger of being abducted for ransom. We interviewed Spanish Red Cross volunteers who helped West African migrants lost at sea, and, in the mortuary, the forensic specialist in charge of the human remains of people who drowned in the Mediterranean and would remain unidentified, leaving their families desperate for news, forever in mourning without closure.

We interviewed Afghan and Pakistani teenagers in Athens who had left their parents and countries behind, fearing for their lives, to cross Iran, Turkey, and the Aegean, treated like hostages by smugglers who confiscated their phones and papers.

We interviewed volunteers at a shelter in an unmarked warehouse, who asked us not to take any pictures of them or to speak about it, as they feared hate crimes and attacks against migrants and those who help them.

With volunteers from the French Red Cross in Calais, we attended a ceremony for those who had sunk and died in Greece, after interviewing Syrians and Sudanese, sleeping in a wasteland and waiting to cross the Channel, with or without life jackets.

We met a nun managing a shelter who had been threatened with death for warning people about the risk of being kidnapped and their families being asked to pay a ransom.

We met security officials who questioned how we would prevent terrorists from using our tool and whether we would let them access the names of people who use it. But we also met law enforcement officers who told us how crucial it was for a trusted and independent organisation to provide these services and alert people to the dangers that could threaten their lives, as messages conveyed by the ICRC would always be more credible than their own.

In Mindanao in the Philippines, we interviewed a displaced community of urban dwellers who could not return to their city, which had been destroyed by the fighting and was now being rebuilt, as records and papers to prove their identity and property rights had been left behind and destroyed.

Summing up, those interviews confirmed what we had imagined before. Needs were multiform. People needed to be assisted with shelter, food, water, medical care, but also connectivity, trusted information, and advice all along their journey and before setting off. Humanitarian agencies could not cope with all these needs. Most of the time, and in the majority of the extremely unsafe areas people fled from and crossed, no humanitarian or government agency could physically access and help them. People often had to rely on themselves, on the information they could receive to make life-or-death decisions, and on the generosity of other people who were also struggling to protect themselves.

In all parts of the world we travelled, we saw an increasing majority of people with smartphones who were asking as a priority for power to charge

them and Wi-Fi to use them. Connectivity was scarce, phones were stolen. People trusted only a tight circle of close friends and relatives, usually only two or three, with whom they shared their intentions and location. Forced to flee to save their lives, they left unprepared and often did not think of saving their contacts or most precious documents. There was a large gap in terms of equipment, literacy, and connectivity between young and old, rural and urban communities. However, for all of them, connectivity and trusted information about their loved ones, about where to find shelter, food, medical care, protection, and the means to protect documents and contacts were essential.

When looking for information online, most of the people we interviewed used a limited number of apps, such as Facebook and WhatsApp. Nearly all the people interviewed were unaware of the multitude of apps, websites, call numbers, or hotlines available from humanitarian and government agencies. Even field staff did not know what their own organisation and others provided online. In one country, we observed that volunteers promoted an app that was no longer available. Looking at the humanitarian digital offering, there were sometimes good websites, clearly informing people of the services provided in one country, but only a few attempts to provide a global response, which in any case remained largely unknown in the field. The information provided online was often fragmented, divided by country, organisation, and service, and was complex to read. Websites of humanitarian organisations often seemed designed for experts, donors, their staff, or the general public, but not for beneficiaries looking for help.

There was room for improvement, starting with our own organisation, but this required a beneficiary-centric approach and, even more challenging, long-term commitment and investment.

The Challenges

Building a Trusted, Helpful, and Widely Used Platform

Adoption and Trust

The adoption of a platform by potential users is a classic challenge for organisations delivering digital services. Companies need to attract and retain the attention of users and convince them that they provide unique value compared with what numerous other apps provide.

Delivering and promoting an app was new to the ICRC and part of our team's learning. We needed to understand its impact, see what led people to download and use RedSafe, see what worked and what did not. When we launched RedSafe, looking at the live data, we saw with great relief that people we did not know, located thousands of kilometres from our Geneva office, had started to download RedSafe. And that trend has not stopped but instead has increased, largely due to a successful promotional campaign.

Then we started to look not only at downloads but at the wider trail of data to understand our impact, question our approach, and improve the solution. The analysis of RedSafe data was key to challenging our assumptions, learning, and improving, but it had to be balanced with the need to protect people's privacy. It also needed to be followed up with a new series of field studies and interviews which we carried out after the launch to assess our pilots and propose improvements.

The adoption of the platform by the ICRC was an even a bigger challenge. We needed to understand the specific issues, challenges, priorities, and organisation of different field delegations and their partners. We then needed to adjust the services RedSafe provided and our approach accordingly. The one-size-fits-all approach would not work. The question was not only how useful this platform would be, but how disruptive it would be for the organisation.

The third challenge we faced was due to the nature of the ICRC's mandate and context. The ICRC works in hostile environments where distrust is the norm. We needed not only to meet people's needs but also to gain the trust of State authorities, law enforcement agencies, communities, and non-State armed groups, with conflicting interests, sometimes fighting each other. We walked a thin line to ensure that the digital services we delivered, the alerts and information we published, the terms we used, and the partners we vetted were not only useful for the people we served but also accepted by all actors as neutral, impartial, and exclusively humanitarian. Pushing humanitarian services in the digital sphere required that we tightly control and limit them and their use, to avoid misuse and preserve the ICRC's reputation.

So, for example, we decided to self-limit the messaging system between users, banning open text, and restricting communications to predefined messages. This limits the risks of misuse and being accused by the authorities of supporting illegal exchanges of content in sensitive contexts, but also diminishes the usefulness, flexibility, and therefore use of this service. We also decided to monitor the vault to ensure that it would not be used to store pictures (such as child pornography) that would run contrary to its humanitarian objective.

A Global Solution but Helpful for Most

Having one global platform focused on humanitarian services had the advantage that users did not have to download different platforms for each country or service. They find in RedSafe the main services and information they need, wherever they are, even when they cross borders.

But having a global and multi-service platform serving many contexts and groups has also raised specific challenges due to the very large diversity of needs, behaviour, languages, levels of literacy, and situations we observed. Could we equally serve the very connected Cubans that we met, the teenagers

from Afghanistan and the Philippines who asked if we could produce videos on TikTok or a game, and the indigenous Guatemalans who barely spoke Spanish and only used WhatsApp? Could we help the person who fled for political reasons and wanted to hide all connections, the many who did not seem to care about protecting their data, and the women who did not want any password to protect their phone access because they said this would make their husbands suspicious?

Cognitive bias could affect us, as well as the people we interviewed. An experienced humanitarian staff member warned us that nearly nobody in Calais had smartphones, but when we went there, all the migrants we met, without exception, had one. This is why we needed to challenge our assumptions, go to the field and check ourselves, compare what people, volunteers, staff, managers, and experts were saying with what we thought, what we saw, and what the usage data and statistics from RedSafe would later reveal.

It took one full year of exploration and reflection, field and technical studies, before we felt ready to start the second part of our journey: the privacy and security by design of RedSafe's foundations and first services.

Building Secure and Independent Foundations

The first challenge for building secure foundations is time and funding. You need to convince sponsors to fund groundwork, which takes time and money, and which nobody sees. Poor groundwork and architectural design will only be revealed once the platform is completed, if the solution stops working or is unable to grow, being too heavy, complex, and costly to maintain. Poor foundations may even be the cause of a data leak. Yet, securing the necessary funds and time to address risks that might never fully materialise can be challenging.

The second challenge is the complexity and long-term consequences of decisions to be made at the start. We had to assess risks and threats in order to come up with the right set of mitigation measures. We had to choose where to host RedSafe, design the right architecture, choose the right set of technologies, and prioritise the services and functionalities we should deliver first.

Talking about independence, security, and privacy-by-design is one thing, but walking this talk in the digital world is much more difficult. It entails a high cost in terms of effort, time, and resources for a result that will never be fully satisfactory.

What do independence and security mean in the digital world, when the systems we use are interconnected but fragile, when its internet backbone and our devices have not been developed with privacy and security in mind, when we depend on a global infrastructure managed by a few states and big tech companies, when incentives to exploit personal data are the main drivers of the new economy, when you also depend on the behaviour, literacy, and

cybersecurity practices of end users, and when you are not a tech company but a humanitarian organisation with limited means and knowledge?

Knowing that it will never be possible to provide a 100% secure digital service, we did our best to limit risks and preserve the ICRC's independence and capacity to act by making six important decisions:

1. Security and privacy were not treated as something to be done only once and forever, but from the start they guided the important decisions we made, from the composition of our team and selection of the company that built RedSafe, to the architecture of the platform, its hosting, encryption, access rights, and the constant design and improvement of services and functionalities. As an example, we hired in our core team a very experienced technological adviser with strong knowledge of security and privacy, who could translate the abstract data protection rules into concrete technical requirements.
2. Before we started to design the solution or choose our main provider and the right set of technologies, we undertook an in-depth analysis of threats, a cyber security risk assessment, a data protection impact assessment, and a legal risk assessment.
3. As a result, we took the important decision not to use commercial clouds, but instead to host RedSafe and all its data on ICRC servers that would be accessed only by ICRC staff. This meant that the ICRC engaged resources and competences to build a secure IT environment that we fully controlled technically and legally. Keeping the solutions on our servers enabled us to benefit from the protection afforded by the ICRC's legal status, privileges, and immunities.
4. We decided to opt for open-source technologies. Open source enabled us to decrease our dependency on major tech providers, which could have been perceived as siding with certain states, with the risk that the solutions the tech companies provided might be under embargo or forbidden to operate in case of tension or conflicts between States.
5. We carried out penetration tests by third parties on a regular basis and, in a first for the ICRC, offered bug bounties to find and patch vulnerabilities. To be forward-looking, we also engaged in R&D, benefiting from the partnership and advice of researchers and academia.
6. We had four years, which is a very long pilot phase, to test RedSafe, first with a limited number of functionalities and in only two regions. Before every new deployment, our global assessments were complemented by specific field assessments. This gave us the time to deliver over four years ten improved versions of RedSafe, to improve its services, our approach, and reinforce RedSafe's security before proposing to use it in other contexts.

RedSafe is a complex platform, as it needs to integrate in one solution different functions provided by different technologies, such as a vault, a messaging system, an interactive map, systems to publish information and alerts, back-up systems for people to register and ICRC staff to manage the platform. No single, off-the-shelf solution can do all this. Therefore, for us to build and operate RedSafe on our servers was a challenge, as it required the ICRC to acquire the resources and competences needed to host, secure, and maintain a combination of new open-source technologies.

Keeping the Flame and Vision

A Five-Year Journey is a Long and Dangerous One

Building a new and secure platform is like building a new and experimental building where you wish to relocate all the front-end services of your global company and safeguard the assets of your clients, without disturbing operations.

If you are not attentive to detail, you might end up delivering windowless rooms, irregular stairways, doors that can be forced open by intruders, and endless construction work that upset your colleagues. When the journey is long, the organisation might change objectives given a change in the sponsors and directors, the ambition to build something new might vanish, key members of the team might leave and be replaced by others who will do things differently, better – in their view, of course. The quality checks and processes which took so long to draft looked great on paper, but will they be followed in the long term if people and priorities change?

The longer the building stays standing, the more you risk that its functions and shape change to match the vision that endorses it. You were supposed to build a school, but it might serve as a hospital due to a change in circumstances. I saw this in Iran, in the ghost town of Khorramshahr, ruined by the war, where, in the early 1990s, I was tasked with leading the transformation of a school that was never used into a hospital for the war wounded. But even that would not be used, as the situation suddenly changed again with the closing of the border, preventing the expected influx of refugees and wounded from Iraq. The perfect building that meets everybody's wishes will look awkward or will never be finished.

So, we aimed at building, first, solid enough foundations and delivering in quick time an initial version of its services, something modular and simple, but safe and attractive enough to be used and tested, and then improved, based upon feedback from users, colleagues, and partners.

The first version of RedSafe was ready to be tested in Southern Africa in May 2021, after one year of development. Four years later, we launched the tenth improved version of RedSafe.

The Team

To help maintain the original vision and navigate the sea of changes, opportunities and risks, the diversity, skills, and endurance of the core team that built RedSafe were essential. I was lucky to hire five passionate, resilient, and skilful team members from diverse backgrounds, who mostly stayed until the end of the pilot phase. Working for several years with the same core team, which had sufficient diversity and autonomy to make decisions, learn, and adjust, was a blessing. It helped to make faster, smarter, but also more consistent decisions by keeping the original vision alive.

The Principles

The other element that served as a compass in troubled waters was the design principles. We defined a set of principles which served as a guiding framework that expressed the values we wished to embody in our platform. They helped us make the right decisions and trade-offs when principles conflicted with each other.

For example, there was a tension between the principle of digital identity (which aimed at identifying users in order to avoid duplication and increase the efficiency of the ICRC and its partners' services) and the two principles of data protection and empowering people. Although it would have been opportune, for the effectiveness of the services provided, to identify all our users, we decided to apply instead a progressive identity framework that minimises the collection of personal data in order to reinforce trust and limit risks. In concrete terms, we enabled people to use most of the services delivered by RedSafe without providing any information about themselves. They only have to authenticate for services that require it (e.g. the vault) to protect their personal data and documents.

Other principles reinforced themselves. The principle of inclusiveness could only be partly satisfied with face-to-face support provided by volunteers who would help people with low digital literacy to register and use the more complex features of RedSafe. It was therefore important to formulate another principle around face-to-face interaction that clearly stated that digital services should not be the only option for people to contact the ICRC and access basic humanitarian services.

Depending on Others

The platform's final shape and functions are the result of a long and largely invisible process, driven by a vision, a long trail made of thousands of micro decisions, which seemed trivial when made, but proved decisive in the end. Progress and benefits also depend on external constraints (such as financial

resources and regulations) and capabilities, which are provided by other sectors of the organisation, as mentioned in these two examples:

1. To build RedSafe, we needed the ICRC's capability to provide us with an efficient IT environment where the digital solutions could be safely developed and tested. While, at the beginning, the release of a new version of RedSafe took a long time, as it required a lot of manual tasks which are more prone to errors, the production of new versions improved with time thanks to better processes and automation.
2. To roll out the RedSafe information as an aid service, we depended upon the capability of each ICRC delegation to appoint staff in a position to vet partners and create and publish information and alerts that meet people's needs but do not cause controversy. This required field knowledge, communication, and diplomatic skills. It was difficult to find them in the ICRC delegations, which had to cut resources following the 2023 financial crisis.[4]

The long-term capacity to collect, verify, and update the trusted information to be published may be the biggest challenge for humanitarian organisations, as this requires the long-term maintenance of a high level of commitment. This is due to the nature of humanitarian work. Humanitarian organisations are more focused on the here-and-now approach, quickly mobilising human resources to physically access and respond to needs in emergencies. They are less accustomed to following a longer-term approach to deliver trusted information online and digital services.

Delivering and managing a digital platform was therefore also an exercise in orchestration between assets we controlled and others (resources, hard and soft skills) we did not.

Conclusion

RedSafe has enabled the ICRC to explore new digital services and better understand their impact and limitations for the people we serve and the organisation itself. We felt that we had no other alternative than to trial it, to take risks ourselves without harming the people who needed assistance and protection. To learn and improve, we needed to explore the unknown and engage in a journey through this brave – and unsafe – new world.

For the people we briefly met and interviewed by the side of the road or railroad, in shelters, in prisons, in wastelands, and in refugee camps, and for

4 See, an update on the ICRC's financial situation: https://www.icrc.org/en/document/update-icrc-financial-situation.

the hundreds of thousands who downloaded RedSafe and we will never meet, there was little more that we could do. After all, what we offered was just an app. But that humanitarian app could – we hoped – help some of them. In conflicts and crises, or when they crossed hostile lands, we believed that RedSafe could help people save their documents and contacts, make life-saving and informed decisions, and find the trusted information and humanitarian services they needed.

We believed that RedSafe could make their own very unsafe journey just a little bit safer.

4

THE LOGIC OF BIOMETRICS AND ORGANISATIONAL ACCOUNTABILITY

Quito Tsui

Introduction

Biometric use within the humanitarian sector emerged in the early 2000s. Initially under the purview of a handful of United Nations (UN) agencies, the use of biometrics then grew steadily across the humanitarian sector. In the mid-2010s, reflection on the use of biometrics increased, as several high-profile incidents implicated the humanitarian use of biometrics. Criticisms began to mount around the technological fallibility of biometrics,[1] the invasiveness of collecting highly personal biological data,[2] and the possibilities of surveillance and exposure, along with the accompanying concerns around the experimentation and privatisation of humanitarian tools,[3] leading several organisations to reconsider their use of biometrics.

The current landscape of biometric use is uneven as organisations have charted individual paths with little consensus or purposeful coherence (see

1 Kerrie Holloway, Reem Al Masri, and Afnan Abu Yahia, "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises," *HPG working paper*, London, 2021, https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises; James Eaton-Lee, "A Responsible Biometric Deployment Handbook," *Simprints*, January 2023, https://uploads-ssl.webflow.com/5a0ad2cbd65a2f0001be3903/64773ad0beced7dd5b6f6d69_A%20Responsible%20Biometric%20Deployment%20Handbook_Final%20(1).pdf.

2 Keren Weitzberg et al., "Between Surveillance and Recognition: Rethinking Digital Identity in Aid," *Big Data & Society* 8, no. 1 (January 2021), https://doi.org/10.1177/20539517211006744.

3 Silvia Masiero, "Digital Humanitarianism: A Critical Discourse Analysis," *MCIS 2023 Proceedings* (Mediterranean Conference on Information Systems, 2023), https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1014&context=mcis2023.

DOI: 10.4324/9781003650164-7

later section on data protection efforts to advance downward accountability). Though the origins of biometric uptake often appear murky, the grounds for continued use are myriad: donor pressure for auditability, reduced resources underpinning deduplication and fraud reduction narratives, and the growing desire for interoperability, all mean continued use of biometrics currently appears inevitable in some capacity as part of humanitarian programming.

Biometric tools sit at the nexus of humanitarian operations, acting as a gateway to services. Across the identity lifecycle, biometric tools are used to register, identify, verify, and deduplicate those receiving humanitarian assistance. They are also part of a wider effort at accountability, providing new pathways for auditing and monitoring the distribution of assistance. While wrestling with external upheaval regarding funding, shifting geopolitics, and increasing hostility towards humanitarians, the sector is also coming to grips with lagging efforts at localisation and shifting power. Related reflections on decolonising the sector add impetus to the consideration of whether and how biometric systems fit with these other currents of change.[4]

This chapter considers the frame of humanitarian accountability and its explanatory capacity for situating the humanitarian use of biometrics. It particularly focuses on the orientation of accountability as furthered by biometrics, considering the contributions of biometrics to both upward and downward accountability. Within the humanitarian sector, humanitarian agencies can be conceived of as having certain "upward" obligations to donors and potentially host nations and "downward" responsibilities to recipients[5] – and as some have argued "sideways" to the wider humanitarian system, e.g. other humanitarian workers or peer organisations.[6] Historical challenges in balancing these different directions of accountability have resulted in humanitarians being accused of prioritising upward accountability to donors to the detriment of downward accountability to impacted communities.[7] This dis-

4 Mirca Madianou, "Reproducing Colonial Legacies: Technocolonialism in Humanitarian Biometric Practices," Contribution to the Expert Workshop on Race, Technology and Borders Convened by the UN Special Rapporteur E. Tendayi Achiume (Office of the United Nations High Commissioner for Human Rights (OHCHR), 2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Mirca_Madianou.pdf.

5 Henrik Buljo Anstorp and Cindy Horst, "Broadening the Concept of Humanitarian Accountability," *PRIO Paper*, Oslo 2021, https://www.prio.org/publications/12760; Erika Baranda and Isabelle Büchner, "Dynamic Accountability: Changing Approaches to CSO Accountability," *Accountable Now*, Berlin, 2019, https://www.csostandard.org/wp-content/uploads/2019/09/Dynamic-Accountability_Accountable-Now.pdf.

6 Dorothea Hilhorst et al., "Accountability in Humanitarian Action," *Refugee Survey Quarterly* 40, no. 4 (2021), https://doi.org/10.1093/rsq/hdab015.

7 Leila Denniston, "'They Just Come and Try to Help' Exploring the Prioritization of Downstream Accountability in Citizen-Led Humanitarianism in Calais," *Citizen Humanitarianism at European Borders*, ed. Maria Gabrielsen Jumbert and Elisa Pascucci

cussion on directions of accountability and biometrics is undertaken noting that upward and downward accountability are not mutually exclusive. Indeed, it is possible for interventions to contribute to both upward and downward accountability. Rather, the chapter is concerned with how the direction of accountability is advanced through current sectoral biometrics. Of special interest is the way biometric use provides insight into the organisational prioritisation or balancing between the two directions.

The analysis finds that biometrics speak predominantly to upward accountability and reinforce established logics of upward accountability. However, this orientation is not static; data protection efforts demonstrate how this logic can be interrupted and how more thoughtful uses of biometrics can be advanced. Data protection regimes broadly provide a framework for accountability that can be mobilised to focus on downward concerns. In particular, when data protection regimes specifically provide details around the conditions of deployment and development of biometric tools, they can help create space for community concerns. When it comes to the use of technology, focused and detailed organisational data protection policies can provide a frontline for accountability and offer a mechanistic path to downward accountability that can otherwise be difficult to institutionalise.

In particular, this chapter is concerned with:

1. A discussion of key tenets of humanitarian accountability and the continued call for accountability to communities;
2. An exploration of how the logic of upward accountability embedded within biometric use intersects with data protection principles and standards;
3. An analysis of the extent to which data protection approaches can provide humanitarians with the tools to address the risks presented by biometric data collection.

Current humanitarian approaches to biometric use are not an inevitability – rather they are the result of calculated data protection choices. By scrutinising how biometric use in the humanitarian sector advances upward accountability, rather than the more downward accountability emphasis of data protection, I intend to contribute to deeper discussions of the needs, limitations, and opportunities for data protection in advancing the interests of impacted communities.

(Routledge, 2021): 66–82; Katja Lindskov Jacobsen, "UNHCR, Accountability and Refugee Biometrics," UNHCR and the Struggle for Accountability, (Routledge, 2016): 159–79, https://doi.org/10.4324/9781315692593-9.

Humanitarian Understandings of Accountability

The impetus to alleviate suffering has mobilised humanitarian action since the sector's inception. Despite this motivation, it has taken humanitarians several decades to address the relationship between their work and those receiving assistance.[8] Humanitarian accountability has been depicted as having both moralistic and mechanistic aspects, with the former speaking to the sector's inception values of humanity, neutrality, impartiality, and independence, while the latter speaks to the legal and procedural efforts at accountability.[9] However, humanitarians have often referenced accountability without agreement on what humanitarian accountability is, leaving overtures to accountability lacking in explanatory power.[10] Efforts to think about accountability in the sector have often divided it into three components: taking account, giving account, and being held to account.[11]

Part of the reason for the dominance of upward accountability is the organising force of donor expectations that requires humanitarians to develop corresponding enabling systems. Although the directions of accountability can co-exist, downward accountability in particular often requires more concerted attention, susceptible as it is to long-standing power dynamics of humanitarian action and the complexities of practically delivering community-driven humanitarian assistance. Consequently, when upward accountability is institutionalised within humanitarian work without corresponding efforts towards clear processes or supporting mechanisms for downward accountability, humanitarians systematically reduce the space for downward accountability. Reporting and evaluation processes have focused on upward accountability and created additional pressure on humanitarians to devise more efficient ways of meeting these expectations, a key pillar of which has been the introduction of biometric tools.[12] Downward accountability has remained amorphous

8 Hilhorst et al., "Accountability in Humanitarian Action".

9 Anstorp and Horst, "Broadening the Concept of Humanitarian Accountability".

10 Y.S. Andrew Tan and Johan von Schreeb, "Humanitarian Assistance and Accountability: What Are We Really Talking About?" *Prehospital and Disaster Medicine* 30, no. 3 (2015): 264–270, https://doi.org/10.1017/s1049023x15000254.

11 Hilhorst et al., "Accountability in Humanitarian Action"; Inter-Agency Standing Committee (IASC), "The Operational Framework," IASC, Geneva, 2010, https://interagencystandingcommittee.org/sites/default/files/migrated/2014-10/AAP%20Operational%20Framework%20Final%20Revision.pdf; Louisa Seferis and Paul Harvey, "Accountability in Crises: Connecting Evidence from Humanitarian and Social Protection Approaches to Social Assistance," *OpenDocs* (Institute of Development Studies), no. 13, (2022), https://doi.org/10.19088/basic.2022.013.

12 Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," *Journal of Intervention and Statebuilding* 11, no. 4, (2017): 529–551, https://doi.org/10.1080/17502977.2017.1347856.

in contrast,[13] fuelled in part by the quantification and datafication impressed upon humanitarian work as a result of upward accountability efforts.[14]

Settling the debate on accountability exceeds the capacity of this chapter. Rather, it is interested in recent shifts towards emphasising downward accountability. In particular, the chapter seeks to understand the implications of biometric use within this growing emphasis on community engagement where accountability becomes more significant given efforts to focus on those who receive humanitarian assistance. Despite its role as probably the most high-profile and extensive initiative mobilising efforts towards downward accountability, the "Accountability to Affected Populations (AAP)" agenda[15] has struggled to produce community-oriented accountability at scale or tackle deeper issues of power within the sector.[16] The feedback on how the AAP agenda has been pursued is especially demonstrative of the audit culture of upward accountability[17] with data generation centred primarily around monitoring and reporting on aid distribution, and ascertaining service-specific feedback on humanitarian action.

Feedback already limits how downward accountability is conceptualised and enacted within humanitarian work, while the shortsightedness of limiting feedback to direct recipients and programmes means there is little room for alternative methods of engagement. Moreover, broader inputs on humanitarian work have no appropriate conduit, meaning the sector has limited understanding of how humanitarian assistance is perceived and received as a whole. The fact that humanitarian comprehension of community experience is fractured is not lost on humanitarians. In recent years, there has been growing acknowledgement of the need to develop more participatory approaches to

13 Sinead Walsh, "Obstacles to NGOs' Accountability to Intended Beneficiaries: The Case of ActionAid," *Development in Practice* 26, no. 6, (2016): 706–718, https://doi.org/10.1080/09614524.2016.1200537.

14 Joël Glasman, Humanitarianism and the Quantification of Human Needs (Routledge, 2020).

15 The UNHCR described AAP as "the commitments and mechanisms that humanitarian agencies have put in place to ensure that communities are meaningfully and continuously involved in decisions that directly impact their lives", in UNHCR, "Accountability to Affected People (AAP)," UNHCR, 12 June 2024, https://emergency.unhcr.org/protection/protection-principles/accountability-affected-people-aap.

16 Theo Tindall, "Beyond Accountability as Feedback: Lessons from Somalia in Holding Humanitarian Responses to Account," *ODI: Think Change*, London, 28 March 2024, https://odi.org/en/publications/beyond-accountability-as-feedback-lessons-from-somalia-in-holding-humanitarian-responses-to-account/.

17 Stephanie Diepeveen, John Bryant, and Mahad Wasuge, "Outsourcing Accountability: Extractive Data Practice and Inequities of Power in Humanitarian Third-Party Monitoring," *Big Data & Society* 12, no. 1 (2025), https://doi.org/10.1177/20539517251328250.

humanitarian work – at times referred to as "shifting power"[18] or "the localisation agenda".[19] Downward accountability in the sector has been driven by practical and principled concern; knowing recipients' experience of the utility of aid can support humanitarians in better calibrating their assistance. Still, these efforts may end up subsumed by the preference for upward accountability measures.

Humanitarianism's moral force can render the margins of accountability uncertain, as it lends a principled value to the seemingly more operational aspects of accountability, such as registration and identification processes. By connecting the characteristics of accountability with its directions, this chapter demonstrates the upward tilt of biometric-based accountability contributions. By assessing humanitarian biometric use against the technology's contributions to "taking account, giving account and being held to account", humanitarians can have a better framework to assess how selected tools contribute to accountability.

Determining the Direction of Biometric-Mediated Accountability

Biometric tools sit at the nexus of humanitarian operations, acting as a key component of access to services. On paper, biometric tools offer the promise of oversight to humanitarians, but the accountability dividends of biometrics are contested and not without concern. Civil society, academics, and humanitarians themselves have raised, *inter alia*, fears about function creep,[20] data protection, privacy, and the risk of surveillance,[21] and the securitisation of biometric data.[22]

How specific technologies contribute to accountability efforts is a growing area of concern.[23] Part of the challenge, however, in analysing biometrics

18 See for example: Rose Worden and Patrick Saez, "Shifting Power in Humanitarian Nonprofits: A Review of 15 NGO Governing Boards," *Centre for Global Development*, 2021, https://www.cgdev.org/sites/default/files/Shifting-power-humanitarian-NGOs-boards.pdf.

19 Emmanuel Viga et al., "Engaging with the Humanitarian Localisation Agenda from 'Below' in Uganda," PRIO Policy Brief, 2024, https://www.prio.org/publications/13953.

20 Vincent Graf Narbel and Justinus Sukaitis, "Biometrics in Humanitarian Action: A Delicate Balance," *Humanitarian Law & Policy Blog*, ICRC, 2 September 2021, https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/.

21 Madianou, "Reproducing Colonial Legacies".

22 Katja Lindskov Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism," ICRC, February 2022, https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.

23 Katja Lindskov Jacobsen and Kristin Bergtora Sandvik, "UNHCR and the Pursuit of International Protection: Accountability through Technology?," *Third World Quarterly* 39, no. 8, (2018):, 1508–1524, https://doi.org/10.1080/01436597.2018.1432346.

with regard to accountability is the differing uses and mandates around the technology. Biometric use includes registration, identity management, and cash and voucher assistance to name just a few – and may at times overlap into functional applications. Additionally, humanitarian contexts vary, with the details of biometric use likely to differ between conflict or displacement contexts. Humanitarian organisations themselves, though part of a collective, may be distinct in terms of the remit of their mandate – UN agencies in particular often have more specific obligations to or operational engagements with state actors. Taken together, there is a need to balance organisationally delineated analysis[24] with efforts to understand sectoral patterns.

The impetus to focus on biometrics within this is threefold: (i) as a frontline technology that members of impacted communities are likely to encounter repeatedly; (ii) the identification properties of biometrics make it a centralising tool within humanitarian work; and (iii) its wide capture of humanitarian work can lock humanitarians into using biometric technology in spite of harms – the UN High Commissioner for Refugees (UNHCR), for instance, has collected some 15.8 million biometric records of refugees,[25] making it logistically challenging to replace a system operating at such scale.

Not all these risks and harms are exclusive to biometrics, and lessons learned extend to the use and introduction of other technologies, making it all the more important to understand how this fundamental technology furthers a logic of accountability that runs counter to humanitarian efforts to concentrate on those who receive assistance. By analysing the way biometrics shape the act of taking account, giving account, and being held to account, this chapter argues that the way biometrics contributes to accountability efforts, and the reason for the contested contributions of biometric tools, lie in its orientation towards upward accountability efforts.

Taking Account

As yet, biometric use has remained outside the remit of AAP and other related downward accountability efforts. Reception to biometric use is not monolithic, with research depicting a highly nuanced picture of how biometric use is perceived by community members. The frame of assessment for individuals engaging with biometric tools often varies; ranging from functionality

24 See, for instance: Çağlar Açıkyıldız, "Unique Data, Different Values: Explaining Variation in the Use of Biometrics by International Humanitarian Organizations," *Global Policy* 15, no. 3, (2024): 502–515, https://doi.org/10.1111/1758-5899.13343.

25 Chris Burt, "UNHCR Adopting Biometric Face Image Quality Standard for Refugee ID Documents," Biometric Update | Biometrics News, Companies and Explainers. BiometricUpdate.com, 17 October 2024, https://www.biometricupdate.com/202410/unhcr-adopting-biometric-face-image-quality-standard-for-refugee-id-documents.

or dysfunctionality to comfort, health, or privacy concerns (or at times lack thereof).[26] Support for, or opposition to, biometrics does not follow a linear path. On the other hand, humanitarian organisations are yet to develop a systematic understanding of how biometric tools are perceived or experienced. An *ad hoc* and piecemeal understanding of biometric use and community reception has thus emerged.

The concept of accountability provides one way to begin analysing biometric use in a more systematic manner. With consultation representing an important aspect of accountability broadly, and of humanitarian conceptions of AAP specifically,[27] the absence of community input in decisions to utilise biometrics demonstrates the primacy of organisations in making that choice. In certain cases, the explicit wishes of community members have been overlooked. Rohingya refugees in Bangladesh organised protests against biometric registration,[28] fearing discrimination along with potential future harms of forced repatriation and denial of citizenship.[29] Additionally, concern expressed by refugees in Kenya and Lebanon regarding data sharing with national governments[30] has not resulted in the cessation of biometric data collection. Refugee concerns about the use of biometrics are sometimes minimised or dismissed.[31]

Continued use of biometrics in the face of anxieties, frustration, or even resistance demonstrates the extent to which organisations may not be sufficiently taking account of how impacted communities understand biometrics. By neither engaging with the substance of concerns nor amending the use of biometrics or the policies governing their deployment, humanitarian organisations cannot be seen to be fully taking account. An absence of either institutionalised involvement or active response to communities when they express distress translates to biometric use that does not include the downward experience of such tools. Revising the assumed use of biometrics is possible: in

26 Weitzberg et al., "Between Surveillance and Recognition".

27 UNHCR, "Accountability to Affected People (AAP)".

28 Suruchi Mazumdar, "Rethinking Digital Humanitarianism in Rohingya Refugee Camps," *Tech Policy Press*, 28 June 2024, https://www.techpolicy.press/rethinking-digital-humanitarianism-in-rohingya-refugee-camps/.

29 Natalie Brinham, "'Genocide Cards': Rohingya Refugees on Why They Risked Their Lives to Refuse ID Cards," *openDemocracy*, 21 October 2018, https://www.opendemocracy.net/en/genocide-cards-why-rohingya-refugees-are-resisting-id-cards/.

30 UN Office for the Coordination of Humanitarian Affairs (OCHA) Policy Development and Studies Branch, "Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies," OCHA, October 2014, https://internews.org/wp-content/uploads/legacy/resources/UNOCHA_Humanitarianism_CyberwarfareAge_PolicyPaper11.pdf.

31 Margie Cheesman, "Infrastructure Justice and Humanitarianism: Blockchain's Promises in Practice," Oxford University Research Archive (2022), https://ora.ox.ac.uk/objects/uuid:3a375a60-85b2-4953-bc04-5cae34021df1.

Ukraine, civil society, citizens, and non-governmental organisations (NGOs) of neighbouring countries contested the use of biometrics, resulting in the humanitarian response being conducted largely without such use.[32] The situations in which organisations take account, and the related geographic variability, suggest that the relative power of local implementers, civil society, and impacted communities plays a role in determining whether, when, and how biometrics is part of a humanitarian response.

Applying an accountability lens to civil society and academic commentary on humanitarian conduct provides another measure of whether or not organisations are taking account. Civil society and academic practitioners calling for organisations to take account have paid particular attention to the way in which biometrics enable surveillance of already vulnerable groups. The extent to which such analysis is included in or excluded from humanitarian reviews of biometric use is another useful measure of the direction of accountability. Biometric tools enable greater end-to-end oversight of impacted communities and the way they interact with humanitarian services. Tracking these engagements, and the movement of individuals across humanitarian systems is, argues Madianou[33] along with Weitzberg et al.[34] and others,[35] tantamount to surveillance. Surveillance possibilities are not limited to humanitarians – biometric use also enables new means for host states and international donors to surveil refugees.[36] Subjecting recipients of assistance to biometric registration within this paradigm is laden with deeper ethical questions about the suspicion engendered by such invasive methods. While civil society and academic critique should not usurp community sentiment, it can provide complementary insights into other relevant ramifications of biometric use.

32 Belkis Wille, "You Don't Need to Demand Sensitive Biometric Data to Give Aid. The Ukraine Response Shows How," *Human Rights Watch*, (2023), https://www.hrw.org/news/2023/07/11/you-dont-need-demand-sensitive-biometric-data-give-aid-ukraine-response-shows-how.

33 Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies," *Television & New Media* 20, no. 6, (2019): 581–599, https://doi.org/10.1177/1527476419857682.

34 Weitzberg et al., "Between Surveillance and Recognition".

35 For discussions of biometric use as tacit and overt surveillance, see: Gus Hosein and Carly Nyst, "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries," *SSRN Electronic Journal*, (2013), https://doi.org/10.2139/ssrn.2326229.

Skyline International, "Biometrics-for-Food: A Dangerous Shift from Humanitarian Relief to Coercive Surveillance," *Skyline International for Human Rights*, 2025, https://skylineforhuman.org/en/news/details/819/biometrics-for-food-a-dangerous-shift-from-humanitarian-relief-to-coercive-surveillance.

36 Çağlar Açıkyıldız, "'I Know You like the Back of My Hand': Biometric Practices of International Humanitarian Organizations in Humanitarian Response," *Disasters* 48, no. 2, (2023), https://doi.org/10.1111/disa.12612.

It is clear then, from such fears and concerns, that widespread use of biometrics does not receive overwhelming support from impacted communities, at least those whose perspectives have been empirically studied.[37] Continued use of biometrics thus begs the question of whose interests are accounted for in its use. Jacobsen argues that biometrics responds to the interests of donors who desire greater accuracy in accounting for refugee populations, and beyond this, to the desire of both states and organisations to experiment with technology in service delivery.[38] American pressure to introduce biometrics,[39] along with allied support for the perceived security associated with biometric identification, were both key drivers of early adoption of biometrics in UN agencies.[40] In this sense, biometrics continues an established pattern of humanitarian experimentation that is notable for being conducted in the absence of community consultation.[41] This upward gaze of biometrics is very apparent when considering taking account as part of accountability.

Giving Account

The clearest space in which to discern the logic of biometric accountability is when considering the ability and efforts of humanitarians to give an account of biometric tools. Deep-seated challenges of auditability and resulting problems of opacity limit the degree to which humanitarians are able to provide "two-way communication with communities that is transparent [and] accessible (culturally, linguistically, technologically)".[42]

The use of biometrics has introduced a new barrier to accessing humanitarian services. In highly adverse environments, operational conditions can

37 Concerns of refugees vary and do not always echo critiques of humanitarian and civil society actors, however, work by individuals such as Margie Cheesman highlights varied concerns and anxieties of refugees related to biometrics, see: Cheesman, "Infrastructure Justice and Humanitarianism".

38 Katja Lindskov Jacobsen, "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees," *Security Dialogue* 46, no. 2 (2015): 144–164, https://doi.org/10.1177/0967010614552545.
Jacobsen, "On Humanitarian Refugee Biometrics".

39 David Martin, "The United States Refugee Admissions Program: Reforms for a New Era of Refugee Resettlement," US Department of State, 4 July 2004, https://2001-2009.state.gov/g/prm/refadm/rls/rpts/36958.htm.

40 Keren Weitzberg, "Machine-Readable Refugees," *London Review of Books, LRB Blog*, 14 September 2020, https://www.lrb.co.uk/blog/2020/september/machine-readable-refugees.

41 Katja Lindskov Jacobsen and Larissa Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care," *Disasters* 43, no. S2 (2019): 151–168, https://doi.org/10.1111/disa.12333; Mirca Madianou, "Technocolonialism, When Technology for Good is Harmful," (John Wiley & Sons, 2024).

42 IASC, "The Operational Framework," 9.

impact the workability of biometric tools, resulting in accidental denial or disruption of services – humidity and dust, for example, can make it difficult for fingerprints to be read properly.[43] By shifting decision-making authority to machines rather than people, organisations have created an inscrutable intermediary that neither aid recipients nor staff can directly argue with. Difficulty in contesting machine-based decisions can result in humanitarian workers themselves being unable to explain why or how decisions are being made.[44] As these operational challenges have surfaced, organisations have formally and informally acknowledged some of the issues and risks associated with biometric use and have worked to minimise these risks from technical and policy perspectives.

Achieving transparency with regard to biometrically mediated decisions may not always be possible. One crucial limitation is the extent to which humanitarian organisations are able to provide insight into or have oversight of privately held tools. Biometric systems frequently involve private sector actors that assist with providing and deploying the technology. Alongside a dynamic of experimentation discussed above, private sector provision of key infrastructural tools such as biometrics has tipped an already delicate scale towards the business of humanitarianism, a context in which humanitarian oversight is eroded. Biometrics reduce the ability of impacted communities to scrutinise the decision-making of either the humanitarian implementers selecting these tools or the private companies creating them.[45] This means that even when humanitarian actors want to provide insights, or when their policies compel them to evaluate vendors, it may in practice not be possible for them to do so. Confidentiality agreements, and other non-disclosure clauses within memoranda of understanding, as well as a lack of access to vetting tools, hamper the relationship of humanitarians with those subject to biometric tools.

As tech companies increasingly embed themselves within the humanitarian sector, they bend humanitarian operations to the particular logic of the tech market, importing the outsourcing and opacity that have enabled tech companies to flourish.[46] While this chapter focuses on the implications of private sector vendors on biometric use, these dynamics do not only manifest

43 Katja Lindsckov Jacobsen, "Humanitarian Technology: Revisiting the 'Do No Harm' Debate," *Humanitarian Practice Network*, ODI, 18 September 2015, https://odihpn.org/publication/humanitarian-technology-revisiting-the-%c2%91do-no-harm%c2%92-debate/.

44 Madianou, "Technocolonialism".

45 Roda Said, "Challenges and Risks Associated with Biometric-Enabled Cash Assistance," *Forced Migration Review*, May 2024, https://www.fmreview.org/digital-disruption/siad/.

46 Quito Tsui, Teresa Perosa, and Samuel Singler, "Biometrics in the Humanitarian Sector. A Current Look at Risks, Benefits and Organisational Policies," *The Engine Room*, 2023, https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf.

in the case of biometrics. Issues of vendor lock-in, for instance, are pertinent more broadly while still being important to note in the biometric use case. Technology companies and other private sector actors, with market-driven motives, may divert humanitarian work away from its own distinct logics.[47] This is fuelled by the relative preparedness of such companies, which can inhibit the space for the discussion and reflection necessary to develop more appropriate and genuinely humanitarian alternatives. The increasingly market-based nature of humanitarian assistance, in tandem with the growing deployment of technology solutions in humanitarian systems, produces a disjointed set of interests, one in which the agency of impacted communities is most vulnerable to being overlooked. The result is a humanitarianism where the needs of impacted humans are secondary to the methods of both market and machine.

Being Held to Account: Humanitarian Responsibility

A perennial struggle of the humanitarian sector has been to hold humanitarians themselves to account. Biometric usage has proven the rule rather than the exception in this case. Clear options for individuals to contest biometric-related decisions are not captured in organisational documentation, and a lack of wider precedent regarding humanitarian accountability leaves impacted individuals with few options for redress.[48] Attempts at remedy where harm has occurred have proven a lengthy process. Double registration in Kenya, where Somali-Kenyan citizens lost their access to citizenship rights after being registered in government and refugee systems, has taken substantial civil society and advocacy efforts to right.[49] Even after more than four years since legal action was started, de-registration is still ongoing.[50] Undoing errors or issues – whether foreseen or accidental – associated with the use of biometric systems is costly for governments, humanitarian organisations, and most of all for the individuals caught between systems. Given the highly context-specific

47 Giulio Coppi, "Mapping Humanitarian Tech. Exposing protection gaps in digital transformation programmes," *Access Now*, 13 February 2024, https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf.

48 Marie-Eve Loiselle, "UNHCR and Biometrics Refugees' Rights in a Legal No-Man's Land?" *Lawless Zones, Rightless Subjects: Migration, Asylum, and Shifting Borders*, ed. Seyla Benhabib and Ayelet Shachar (Cambridge: Cambridge University Press, 2025): 228–244, https://www.cambridge.org/core/books/lawless-zones-rightless-subjects/unhcr-and-biometrics/CD8E625C4E7119518610D35FE977D85E.

49 Wangui Gitahi, "Navigating the Legal Landscape of Double Registration in Kenya," *Forced Migration Review*, 20 August 2024, https://www.fmreview.org/digital-disruption/gitahi/.

50 Stephen Astariko, "State given 60 Days to Deregister Kenyans from Refugee Database," *The Star*, 23 January 2025, https://www.the-star.co.ke/counties/north-eastern/2025-01-23-state-given-60-days-to-deregister-kenyans-from-refugee-database.

nature of humanitarian operations and biometric use, it is likely that righting biometric-facilitated wrongs will remain a lengthy process. Without clear systems for complaint and adjustment, impacted individuals will only continue to suffer.

Biometric use speaks to the emphasis on data collection within humanitarian efforts, a sentiment Antonio Guterres embodied when he described data as "the lifeblood of good policy and decision-making".[51] The concurrent 'outsourcing' of accountability to third-party monitors has contributed to an environment of increased data collection and sharing.[52] This does not mean that the use of biometrics has met donors' need for assurances regarding duplication of aid or beneficiary fraud. Preliminary research, along with insights shared in more than 15 different key informant interviews, suggests that the most substantial fraud and corruption in terms of fiscal amount is likely to occur upstream, especially during procurement or as a result of aid diversion[53] – a problem that the dominant application of beneficiary biometrics does not address.[54] Despite this misalignment, continued use of biometrics suggests that appealing to the pretence of donor assurance has been prioritised over addressing ongoing and emerging harms related to the use of biometric systems. Meanwhile, donor interest in interoperability for deduplication[55] has also meant that less risky applications of biometrics (verification rather than identification) cannot be pursued.[56] Safer versions of biometrics, such as tokenisation, which inhibits reverse identification by replacing sensitive information with other information,[57] cannot be used for deduplication

51 OCHA, "Responsible Approaches to Data Sharing – Guidance Note Series: Data Responsibility in Humanitarian Action," December 2020, https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/9db86627-8d8b-435f-8455-6c02802f8fee/download/guidance-note-8.pdf.

52 Diepeveen et al., "Outsourcing Accountability".

53 Jamie Bergin, Sabrina White, and David Jackson, "Corruption in Humanitarian Assistance in Conflict Settings," 2024, https://knowledgehub.transparency.org/assets/uploads/helpdesk/Corruption-in-humanitarian-assistance-in-conflict-settings_2024_Final.pdf.

54 Holloway et al., "Digital Identity, Biometrics and Inclusion"; Quito Tsui and Linda Raftree, "Alternatives to Biometrics for Deduplication," (unpublished manuscript, 2024).

55 Robert Worthington and Andrea Duechting, "USE CASE 1 Deduplication of People, Families or Households," *Cash Hub* (IFRC, 2023), https://cash-hub.org/wp-content/uploads/sites/3/2023/05/DIGID-Interoperability-Deduplication-of-people-families-or-households.pdf.

56 Quito Tsui et al., "Data Sharing in Humanitarian Cash and Voucher Assistance (CVA): A Look at Risks, Threats and Mitigation Technologies," *Relief Web*, NRC, 23 November 2023, https://reliefweb.int/report/world/data-sharing-humanitarian-cash-and-voucher-assistance-cva-look-risks-threats-and-mitigation-technologies.

57 James Eaton-Lee, "A Responsible Biometric Deployment Handbook," (Simprints, 2023).

applications as the substitution method of tokenisation is mutually exclusive from the linkability necessary for identification.[58]

The response of the sector as a whole to potential and realised risks is one indicator of the willingness or facilitation of being held to account. Claims of biometric benefits have undergone limited interrogation, and a relative lack of attention and consideration has been paid to the risks and harms for communities. The uneven burden of risk and harm demonstrates once more the prioritisation of upward accountability needs over the problems of access. These trade-offs do not need to be explicit or purposeful; humanitarians are often in a difficult bind, reliant as they are on donor support to continue their operations. Ignoring, however, the one-sided interaction furthered by biometrics evidences the humanitarian emphasis on donors and upstream actors when deploying biometric tools. Biometrics render recipients accountable to organisations, while leaving communities with few mechanisms to hold humanitarian agencies accountable when biometric-related challenges and harms do arise.

Taking a step back from responding to actual harm, we can also consider the sector's (un)readiness to mitigate potential harm as another indicator of willingness to take responsibility for the kind of risks biometric-related humanitarian decisions may introduce. Here we turn to data protection efforts to unpack how humanitarians have conceptualised risk by exploring attempts at risk mitigation.

Data Protection Efforts to Advance Downward Accountability

Humanitarian data protection establishes a critical link between responsible custody of sensitive data and the preservation of dignity. For those who interface with humanitarian services and entrust organisations with their data, proper protection is a critical aspect in safeguarding trust between organisations and recipients.[59] As a datafied representation of an individual, biometrics, perhaps more than other data collected, create a digital facsimile of a registrant's humanity. Consequently, as a mechanism of downward accountability, thorough data protection policies providing critical protections are a

58 Justinas Sukaitis, "Building a Path towards Responsible Use of Biometrics," EPFL, 15 April 2021, https://infoscience.epfl.ch/entities/publication/25fd708e-a297-4f27-bf96-1a42838cfb39.

59 IFRC, "Data Protection," IFRC, n.d., https://www.ifrc.org/our-promise/do-good/data-protection; ICRC, "Safeguarding Humanitarian Data: Power of Humanity Council of Delegates of the International Red Cross and Red Crescent Movement," Council of Delegates of the International Red Cross and Red Crescent Movement, 2022, https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf.

manifestation of the fundamental humanitarian principles and the dual duties of 'do no harm' and a responsibility to protect.

This section considers how humanitarians have approached biometric data protection while also considering the opportunities and limitations of the ability of data protection efforts to introduce downward accountability to the use of biometrics.

Biometric Related Data Protection Policies

There are few comparative studies of data protection policies vis-a-vis biometrics. As a result, there is also limited understanding of how different data protection policies address, mitigate, or, in some cases, overlook the risks related to biometric use. Previous research has noted the lack of clear, publicly accessible data protection policies that provide detailed instruction on the use or deployment of biometrics.[60] More common is the use of data protection policies that consider biometrics as one instance of sensitive data that warrants a higher order of protection.[61]

Oxfam and the International Committee of the Red Cross (ICRC) are well-known examples of strong and detailed biometric policies. The ICRC policy uses public interest for activities such as its Restoring Family Links programme, where the ICRC has a mandate to identify people. On the other hand, where no such mandate exists, for instance, for beneficiary management and aid distribution, legitimate interest is used as the basis for biometric use, determining biometric application through a balancing exercise that weighs the benefits of use against potential risk.[62] Meanwhile, Oxfam, following a moratorium on the use of biometrics, released an updated biometric policy that outlines an "ethics and harms-based approach" that emphasises practical guidance around what "good" biometrics looks like.[63] In their policies, Oxfam and the ICRC have highlighted the potential risks borne disproportionately by impacted communities, finding on balance that the risks to such communities are too great compared to the operational gains. As a result, their policies reflect a more restricted approach. *Médecins Sans Frontières*

60 Tsui et al., "Biometrics in the Humanitarian Sector".

61 Belkis Wille, "The Data of the Most Vulnerable People Is the Least Protected," *Human Rights Watch*, 11 July 2023, https://www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected.

62 Ben Hayes and Massimo Marelli, "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy," *Humanitarian Law & Policy Blog*, 18 October 2019, https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.

63 James Eaton-Lee and Elizabeth Shaughnessy, "Oxfam's New Policy on Biometrics Explores Safe and Responsible Data Practice," *Views & Voices*, 24 June 2021, https://views-voices.oxfam.org.uk/2021/06/oxfams-new-policy-on-biometrics-explores-safe-and-responsible-data-practice/.

(MSF) followed a similar approach to the ICRC and Oxfam of weighing up the risks and benefits. Unable to find a sufficiently compelling reason to use biometrics, and given the risks MSF deemed biometrics to introduce, the organisation decided to forego its use altogether.[64]

The ICRC and Oxfam saliently make suggestions as to what biometric systems would be able to meet their standards. Notably, the ICRC discusses a data protection-focused approach to biometric use[65] that deploys biometrics for verification rather than identification, with the latter being more likely to expose registrants to risk due to the linking of identifying biographical information with identifying biometric information. The ICRC's decision to use biometrics for verification rather than identification results from the ability to use verification in a safer tokenised format.[66]

Data Protection Without Biometric Specific Policies

Other important humanitarian players in the biometric space, such as UNHCR and the World Food Programme (WFP), do not have a publicly available biometric policy. UNHCR's General Policy on Personal Data Protection and Privacy (GDPP)[67] and WFP's Guide to Personal Data Protection and Privacy[68] are briefer in their discussion of biometrics, including it as part of a broader data protection policy as an example of sensitive data. This gives some insight into specific operational requirements regarding the processing of data designated as such. Some agencies have taken a different path and evaluated biometric-related risks as part of broader attempts to think about potential data protection risks. World Vision has cautioned against the use of biometrics,[69] and the UN Children's Fund's (UNICEF) 'Faces, fingerprints and feet'[70] provides a comprehensive, although not binding, overview of the appropriate use of biometrics. Others have commissioned and shared work on the potential

64 Açıkyıldız, "Unique Data, Different Values".

65 Boya Wang et al., "Not yet Another Digital ID: Privacy-Preserving Humanitarian Aid Distribution," *ArXiv* (IEEE Symposium on Security and Privacy (SP), 2023), https://arxiv.org/abs/2303.17343.

66 Kasra EdalatNejad et al., "Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution," *ArXiv*, Cornell University, (2023), https://doi.org/10.48550/arxiv.2308.02907.

67 UNHCR, "General Policy on Personal Data Protection and Privacy | Refworld," Refworld, 2023, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207.

68 World Food Programme, "WFP Guide to Personal Data Protection and Privacy," 2016.

69 Açıkyıldız, "Unique Data, Different Values".

70 UNICEF, "Faces, Fingerprints & Feet Guidance on Assessing the Value of Including Biometric Technologies in UNICEF-Supported Programs" (UNICEF, July 2019).

implications of biometrics, though again they have not necessarily altered or developed policies in response to the risks highlighted.[71]

These data protection policies do go some way to inviting downward accountability, specifically by contributing to the element of being held to account. Data protection policies stipulate processes in the event of data breaches or other adverse uses of data, and designate individual roles and responsibilities for data-related supervisors, including data protection officers, data controllers, and data protection focal points – the latter of which has been introduced by both UNHCR and the ICRC.[72] However, the next stage is for these organisations to find ways to mobilise the reporting mechanisms of their data protection policies to make it clearer for impacted communities to know how they can exercise their rights.[73]

Re-Orienting the Logic of Biometric Accountability

Humanitarian governance is a critical conduit for downward humanitarian accountability. Biometric-specific policies and data protection discussions empower both organisations and community members by taking a clear step towards giving account of and being held to account for technological decisions. For instance, clear instruction on the responsible conditions for biometric use and reflection on the routine use of identity management within this contribute to giving account of how critical tech-related decisions are made. Equally, having public disclosure of biometric policies enables greater transparency – organisations cannot be held to account if external actors, such as members of impacted communities and civil society, do not know the conditions under which biometric tools are being used.

This is why, although data protection policies classify biometrics as a type of sensitive data, there are still shortcomings in this more truncated approach to biometric use-related policies. The key distinction between protections derived from biometric-specific policies and from data protection is twofold: first, the lack of specificity gives wide purview to implementation, and a higher chance of unsafe, or at the very least inconsistent, use. Second, the downward

71 Linda Raftree, "Digital Safeguarding for Migrating and Displaced Children: Practical Next Steps for the Aid Sector" *Save The Children*, 2021, https://savethechildren.ch/wp-content/uploads/2021/11/Digital-Safeguarding-for-Migrating-and-Displaced-Children.pdf.

72 See, for instance, the new Article 27b introduced by the 2025 update of the ICRC Rules, which establishes Data Protection Relays as designated focal points within the organisation to support the implementation of data protection responsibilities at field and headquarters levels. ICRC, "ICRC Rules on Personal Data Protection," International Committee of the Red Cross, 10 April 2025, https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

73 Loiselle, "UNHCR and Biometrics Refugees' Rights in a Legal No-Man's Land?".

accountability dividends are not equal. Explicit policies about when it is legitimate to use a biometric system – or indeed if it is legitimate at all – are a way for organisations to be proactive in holding themselves accountable to communities. By reckoning with the potential repercussions of biometric use and actively considering benefits in direct relation to the risks, organisations can take steps to hold themselves to account and potentially delimit their use of biometrics. Reflecting on biometric-related risks has resulted in circumscribed use of biometrics for MSF, Oxfam, and the ICRC. Comparisons between organisations that have done the work of sharing their rationale around biometric use and those which have not or are utilising data protection policies to cover biometric use demonstrate important gradations in the ability of data protection to advance downward accountability.

Notably absent is the act of taking account and actively engaging with participants. Participation, though much talked about, has frequently eluded humanitarians. Academics and civil society have undertaken the brunt of the work on this, attempting to capture the ways in which biometric use generates different concerns, ranging from health,[74] to surveillance and data extraction,[75] and even longer-term fiscal impediments such as challenges in accessing loans.[76]

Data protection is therefore a necessary but insufficient condition for enabling greater downward accountability. Crucially, the policy focus of data protection can create space for operational practice that formalises the rights of impacted communities to have a say in the services they receive and the technologies used in service delivery. The case of biometrics shows how organisations can build on data protection efforts to delineate biometric-specific policies, enabling a more holistic approach to accountability that challenges the default upward trajectory of accountability analysis. Detail in particular serves an important function in this reorientation; additional policy formulation has resulted in organisations being better able to explain to communities the motivation for biometric use and has placed greater importance on a deliberative stance towards biometric data. A layered approach makes it more likely that data protection work advances downward accountability.

74 Cheesman, "Blockchain for Refugees," *Medium*, 9 June 2022, https://medium.com/data-society-points/blockchain-for-refugees-a46b41594eee.

75 Martin Lemberg-Pedersen and Eman Haioty, "Re-Assembling the Surveillable Refugee Body in the Era of Data-Craving," *Citizenship Studies* 24, no. 5, (2020): 607–624, https://doi.org/10.1080/13621025.2020.1784641.

76 Quito Tsui et al., "Data Sharing in Humanitarian Cash and Voucher Assistance".

Emerging technologies such as artificial intelligence (AI) – generative and otherwise,[77] low Earth orbit communication tools,[78] expanding identity and registration systems,[79] as well as data stewardship pilots[80] are all new frontiers of humanitarian work that may introduce new accountability quandaries. Here, data protection as an active practice can offer space to interrogate the direction of accountability embedded within these new tools. This can in turn be used to inform more specific or detailed policy on the kind of limitations or mitigations relevant to particular technologies. A specific barometer of accountability can offer a litmus test for the degree to which organisations are utilising data protection as a space to formalise accountability to the communities they engage with. Holistic accountability requires actively countering the uneven power dynamics that mean upward accountability tacitly dominates the way accountability is conceptualised – and by extension then how tools and technologies are assessed. Data protection is thus an opportunity that organisations must mobilise to fully extract a contribution to downward accountability.

Advancing the Downward Accountability Possibilities of a Data Protection Approach to Biometrics

Assessing individual organisational data protection approaches is one facet of understanding how data protection can be part of enhancing downward accountability in biometric use. Another key aspect of this is the overarching sectoral approach that currently has significant gaps.

The lack of shared standards was mentioned earlier in this chapter, but there are other gaps to address. As part of being held to account, humanitarians

77 Sarah Spencer, "Humanitarian AI Revisited: Seizing the Potential and Sidestepping the Pitfalls," vol. 89 (London: ODI, 2024), https://odihpn.org/wp-content/uploads/2024/05/HPN_Network-Paper89_humanitarianAI.pdf; Giulio Coppi, Rebeca Moreno Jimenez, and Sofia Kyriazi, "Explicability of Humanitarian AI: A Matter of Principles," *Journal of International Humanitarian Action* 6, no. 1, (2021), https://doi.org/10.1186/s41018-021-00096-6; Active Learning Network for Accountability and Performance (ALNAP), "Explain Briefing: AI in the Humanitarian Sector," ALNAP, 19 May 2025, https://alnap.cdn.ngo/media/documents/ALNAP-EXplain-EssentialBriefings-LongRead-AI_5Ebyny0.pdf.

78 Aaron Martin and Quito Tsui, "Humanitarian Connectivity in Crisis," *Global Policy Blog*, 2025, https://www.globalpolicyjournal.com/blog/02/06/2025/humanitarian-connectivity-crisis.

79 Emrys Schoemaker, Aaron Martin, and Keren Weitzberg, "Digital Identity and Inclusion: Tracing Technological Transitions," *Georgetown Journal of International Affairs* 24, no. 1, (2023): 36–45, https://doi.org/10.1353/gia.2023.a897699.

80 See, for example, the work of Amos Doornbos and the Collaborative Cash Delivery Network: Amos Doornbos, "Emerging Models of Data Stewardship for People Affected by Crisis," *This Is Amos*, 23 February 2023, http://thisisamos.com/emerging-models-of-data-stewardship-for-people-affected-by-crisis/.

need to grapple with the implications of biometric use and the broader challenges that accompany such use. Vendor lock-in and reliance on external suppliers for proprietary software can leave humanitarians unable to properly give an account, and it can also mean, in the event of wrongdoing or mistakes, that liability is unclear, creating uncertainty about who should be held to account.

Once data is collected, it is difficult to deny access, particularly where there are legal requirements that mandate disclosure,[81] meaning that organisations may find themselves in the inevitable position of sharing data regardless of the preferences or concerns of impacted communities.[82] This is why scrutinising data collection processes in advance can strengthen future organisational positions**.** Forward-looking preparation is vital to ensuring data protection in the long term while also serving as an important check on over-collection and excessive retention of beneficiary data. The current lack of discussion on the ramifications of organisations being unable to afford the cost of proper security measures now and in the future could mean humanitarians find themselves unable to maintain systems in the long run.

As both technologies change and the wider data protection landscape shifts, humanitarians need to be cognisant of whether they are able to keep pace with change. Biometric use has often outstripped policy making; placing a moratorium on use, as in the case of Oxfam, can provide the space to tackle the new risks and the uncertainty that accompanies new tools. Emerging frameworks of data management, such as data stewardship, offer humanitarians insight into accountability models that enable greater individual autonomy over information, potentially disrupting the current mode of organisational control over data.

Conclusion

Humanitarian data protection is an ongoing effort that is by no means perfect. However, its ability to contribute substantially to redirecting biometrics towards protecting impacted communities and ensuring safe and purposeful use of biometrics should not be overlooked. Against a backdrop of inconsistent biometric use, humanitarians need to have a firmer grasp on data protection for biometrics. Though data protection is not a panacea for the risks of biometrics, it is a tool that can play a role in directing the accountability logic of technologies such as biometrics.

This chapter has demonstrated the importance of interrogating accountability claims regarding technological tools, and the need to ascertain the

81 Sean McDonald, "From Space to Supply Chains: A Plan for Humanitarian Data Governance," *SSRN Electronic Journal* (2019), https://doi.org/10.2139/ssrn.3436179.

82 Jacobsen, "On Humanitarian Refugee Biometrics".

direction of accountability that a tool facilitates. Further it is argued that when measured against three distinct aspects of accountability – taking account, giving account, and being held to account – biometric use has a distinct proclivity towards supporting upward accountability. In turn, this chapter has shown how data protection can be, and has been, a key tool in directing the accountability logic of biometrics, while articulating the limitations of over-reliance on data protection to facilitate downward accountability. Where data protection approaches to biometrics elaborate clearer conditionality and implement a degree of restriction on its use, their contributions towards enhancing downward accountability are greater. A more discerning biometric approach is one that is informed by risk and built on an explicit comparison between biometric and non-biometric options.

Countering the instinctive upward focus of biometric use requires organisations to be more open about the purpose of biometrics. When left unchecked, the momentum of biometrics tracks towards upward accountability. Moving forward, humanitarians need an approach to biometrics that accounts for the burden of vulnerability: that is, an explicit discussion of how impacted communities most directly experience these harms while benefiting the least from the hoped-for benefits of biometrics.

PART 2.2

Understanding the Digital Transformation of the Humanitarian Space through Data Protection

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

5

DIGITAL TRANSFORMATION AND THE HUMANITARIAN-DEVELOPMENT TRANSITION

The Role of Digital Public Infrastructure and Data Protection

Emrys Schoemaker and Aaron Martin

Introduction

The humanitarian system has made commitments in the Grand Bargain to strengthen the transition in the humanitarian-development nexus from humanitarian aid to longer-term, locally-led responses – including through a greater role for host States in the provision of relief and services. While the emphasis on this transition has grown – particularly in the context of a severe decline in humanitarian aid – the role of digital technologies, systems, and data in this transition has not received the attention it needs.

Humanitarian response is increasingly digital, with systems transforming and digital cash serving as a significant part of that response. However, despite this increasingly digital and data-oriented form of humanitarian response, the implications of digitalisation have not received significant attention in debates about the transition of humanitarian aid and services. In the face of increasing demands for efficiencies, integration, and transformation, this chapter examines how one approach to the digital transformation of service delivery may offer opportunities, while also highlighting the underlying challenges in the transition between humanitarian and longer-term, locally-led development responses.

Digital public infrastructure (DPI) is an approach to digital transformation that promises efficiency savings and a more joined-up, integrated approach to building the 'digital rails' on which public services are delivered. At its core, DPI is characterised by digital identity, payment and data exchange systems – the core systems that public services as well as humanitarian response depend on. A 'pure' DPI sees singular systems shared across government, enabling a fragmented public sector to achieve efficiencies and innovation through

DOI: 10.4324/9781003650164-9

greater integration – much as the humanitarian sector is being called upon to do.

Through research conducted with humanitarian stakeholders on more integrated approaches to management information systems (MIS) in humanitarian aid, this chapter suggests that most view efficiency as the main driver of such approaches to transformation. It also highlights the concerns that many raise around the protection of data in such a more integrated approach and explores the implications of integrated systems for the protection of humanitarian principles and 'humanitarian space'. It discusses how the principles and policies that govern data management and protection are rooted in these same commitments. It argues that the exclusive purpose specification of data collected for humanitarian relief both protects humanitarian space and is threatened by the transfer of data to other actors for purposes other than the humanitarian response. The chapter concludes by looking forward in order to explore what a DPI approach would need to consider in order to maintain humanitarian principles and humanitarian space, exploring specific privacy-protective approaches and technologies that can enable the transition of humanitarian aid and relief and yet protect the core principles on which humanitarian response is built.

The Humanitarian to Development Transition

The humanitarian-development nexus represents a conceptual framework aimed at bridging the traditional divide between short-term humanitarian assistance and longer-term development efforts. This nexus has gained significant traction as protracted crises, a competitive funding context, and a growing number of actors who are active in both humanitarian and development work have led to a blurring of the distinction between immediate emergency response and sustainable development work.[1]

The concept of the humanitarian-development nexus emerged from the recognition that the traditional models of humanitarian relief and development, designed for either only short-term responses or longer-term development, were insufficient to address the protracted crises that now account for the majority of humanitarian activity.[2] Although the idea of linking humanitarian relief to broader development has a long history,[3] the 2016 World

1 Atsushi Hanatani, Oscar A. Gómez, and Chigumi Kawaguchi, eds. *Crisis Management Beyond the Humanitarian-Development Nexus* (London: Routledge, 2018), https://doi.org/10.4324/9781351006828.

2 Sonja Hövelmann, "Triple Nexus to Go: Humanitarian Topics Explained," *Berlin: Centre for Humanitarian Action*, 2020, https://www.chaberlin.org/wp-content/uploads/2020/03/2020-03-triple-nexus-to-go-hoevelmann-en.pdf.

3 Hövelmann, "Triple Nexus to Go".

Humanitarian Summit marked a pivotal moment in formalising this approach. One outcome of this was the Grand Bargain, a series of commitments including an emphasis on and commitment to collaborative efforts across the humanitarian, development, and peace sectors. A core goal of these commitments was to move beyond purely reactive emergency responses towards more proactive and sustainable solutions.

The Grand Bargain commitments to strengthening engagement between humanitarian and development actors included a number of specific goals, including shrinking humanitarian needs over the long term with a view to contributing to the achievement of the Sustainable Development Goals. It also included a commitment to increase the preparedness of aid organisations and donors, as well as national governments and the private sector. There were commitments to longer-term, durable solutions, as well as to increase social protection programmes, to strengthen national and local systems, and to establish new partnerships with multilateral development banks and the private sector.[4]

These are ambitious policy goals for transitioning support, financing, and power to local and national actors, including to the States that host recipients of humanitarian relief. The nexus of humanitarian and development activities has led some to identify a transition as a conceptual approach and policy goal of shifting services and support from international humanitarian actors to local humanitarian and development actors, including host States.

The idea of the nexus has historically been described variously as a "bridge",[5] a "continuum",[6] or even a "triple nexus"[7] (incorporating peacebuilding in addition to humanitarian response and development). Within the efforts of the Grand Bargain, the workstream around the nexus began with some momentum, but faced with the sheer scale of the Grand Bargain's scope and ambition, there was concern amongst the signatories that the overall agenda required streamlining, and that the nexus agenda was also already served by other policy processes, including within the Organisation for Economic Co-operation and Development's Development Assistance Committee (OECD-DAC) and in relation to the United Nations (UN) Reform Process and the New Way of Working.

4 International Council of Voluntary Agencies (ICVA), "The Grand Bargain 2.0 Explained – An ICVA Briefing Paper," 2022, accessed 11 June 2025, https://www.icvanetwork.org/resource/the-grand-bargain-2-0-explained-an-icva-briefing-paper-2022/.

5 Alexander Kocks et al., "Building Bridges Between International Humanitarian and Development Responses to Forced Migration," (Stockholm: EBA, 2018), https://nbn-resolving.org/urn:nbn:de:0168-ssoar-58565-6.

6 Joanna Macrae and Adele Harmer, "Beyond the Continuum: An Overview of the Changing Role of Aid Policy in Protracted Crises," *Research Briefing* (London: HPG, 2004), https://media.odi.org/documents/279_GpS59wf.pdf.

7 Hövelmann, "Triple Nexus to Go".

Thus in 2018, the co-conveners took the decision to close the workstream and mainstream the commitments across other workstreams. In 2021, five years after the Grand Bargain was established, signatories reviewed the scope and structures, and established a new 'Grand Bargain 2.0' that focused on two mutually reinforcing 'enabling priorities': quality funding and localisation/participation,[8] with continued commitments to strengthen anticipatory action, financing mechanisms, and the nexus. In 2023, the signatories to the Grand Bargain again reviewed progress and agreed a Grand Bargain 3.0 framework for 2023–2026 that represents a strategic narrowing from the original 51 commitments to a more focused approach, but one that includes 'practical' policy goals[9] around anticipatory action, innovative ways of financing, and the humanitarian-development nexus, which it was hoped would stimulate engagement from actors beyond the humanitarian system.[10] While the role of the nexus has evolved in the Grand Bargain, it has returned as a core theme of the latest round of commitments to aid reform, ensuring its centrality to the way humanitarian assistance is delivered.[11] Yet while the nexus remains a central concept within discussions around humanitarian aid delivery, the term conceals a diversity of perspectives in the way different actors perceive the relationship between the fields of humanitarian and development activity.

Institutional perspectives often frame the nexus primarily as a coordination challenge. The OECD-DAC recommendation on the (triple-)nexus emphasises "complementarity", "coherence", and "collaboration" across humanitarian, development, and peace actors while "respecting humanitarian principles".[12] Similarly, the UN Inter-Agency Standing Committee (IASC) commonly describes the nexus as an opportunity to align planning and programming approaches to achieve "collective outcomes".[13] In other words, for the aid community, particularly donors and multilateral aid organisations, the nexus is framed as a response to changes in the context of crises, the inadequacy of existing international systems, and inefficiency and fragmentation in humanitarian and development response.

8 Victoria Metcalfe-Hough et al., "The Grand Bargain in 2021: an independent review," *ODI*, London, 2021, https://odi.org/en/publications/the-grand-bargain-in-2021-an-independent-review/.

9 Irwin Loy, "Why the Future of Grand Bargain Aid Reforms Hinge on Accountability," *The New Humanitarian*, 15 October 2024, https://www.thenewhumanitarian.org/news/2024/10/15/why-grand-bargain-future-hinges-accountability.

10 Loy, "Why the Future of Grand Bargain Aid Reforms Hinge on Accountability".

11 Active Learning Network for Accountability and Performance (ALNAP), https://alnap.org/help-library/focus-topics/humanitarian-development-peace-nexus/.

12 OECD, "DAC Recommendation on the Humanitarian–Development–Peace Nexus," *OECD*, Paris, 2019, https://legalinstruments.oecd.org/en/instruments/oecd-legal-5019.

13 IASC, "Light Guidance on Collective Outcomes," *IASC*, 2020, https://reliefweb.int/report/world/iasc-policy-light-guidance-collective-outcomes-june-2020.

On the other hand, critics have challenged these framings. Critical scholars have instead suggested that the language of the nexus often represents "old wine in new bottles",[14] reframing enduring challenges such as resource and capacity constraints instead of engaging with structural causes, such as the tensions arising from differences between humanitarian and development mandates. Others argue that the idea of the nexus is driven primarily by the UN and donors,[15] and reflects longstanding donor preferences for integrated approaches rather than any demonstrable benefits.

Yet perhaps the most fundamental tensions at the heart of the nexus are competing ideas about crisis response and international assistance. While some view the nexus as an approach towards strengthening State institutions, others see it as primarily about improving technical coordination that maintains a necessary separation between humanitarian and development activity.[16]

These tensions remain unresolved and will only increase in the face of the most severe funding crises the humanitarian and development sectors have faced.[17] With the United States cutting its humanitarian and development support and other States following suit, and the UN facing a severe financial crisis, there have been and will continue to be extensive cuts to humanitarian response. As a result, humanitarian organisations are retreating from a number of crises, leaving development actors and host States as the default institutional actors. These changes have also come at a time of discussion about a comprehensive agenda of UN system reform which proposes to streamline operations and realign mandates as a direct response to the financial crisis that is squeezing the organisations.[18] This streamlining includes a discussion of merging separate organisations into 'clusters', for example of humanitarian agencies, and a focus on more integrated approaches to the response to essential needs and delivery of services. Whether these lead to a contraction of humanitarian and development aid from the linkages between the two, or increased interest in finding efficiencies through shared systems and services,

14 Dan Gudgeon and Dong Jin Kim. "Old Wine in New Bottles? A Triple Nexus Approach to Linking Aid Cooperation to Peacebuilding on the Korean Peninsula," *International Peacekeeping* 32, no. 1 (2025): 73–97, https://doi.org/10.1080/13533312.2024.2425653.

15 Hövelmann, "Triple Nexus to Go".

16 Hövelmann, "Triple Nexus to Go".

17 International Rescue Committee (IRC), "Global Aid Crisis: 13 Countries Most Affected by International Aid Cuts," accessed 17 June 2025, https://www.rescue.org/13-countries-impacted-aid-cuts.

18 Jordan Ryan, "UN80 and the Reckoning Ahead: Can Structural Reform Deliver Real Change?" *IPI Global Observatory* (blog), 8 May 2025, https://theglobalobservatory.org/2025/05/un80-and-the-reckoning-ahead-can-structural-reform-deliver-real-change/; Erica Harper, "UN Reform: Where to Cut, How to Save, and the Need for Smart Reform," *The New Humanitarian*, 8 May 2025, https://www.thenewhumanitarian.org/opinion/2025/05/08/un-reform-where-cut-how-save-and-need-smart-reform.

the implications for the relationship between humanitarian and development activities will be profound.

The nexus thus represents a critical policy and operational framework for the way humanitarian relief efforts are conceived, designed, and organised, and the way humanitarian services are delivered. This operational vision, and its implications for the transition of service delivery from humanitarian to development and State actors, raises significant challenges in terms of the digital systems and data used to deliver services, and the protections they are afforded.

Digital systems and data are increasingly central to contemporary humanitarian response.[19] They offer the promise of delivering relief in a fast and cost-effective manner, delivering efficiencies and scale – from enabling connectivity, strengthening early warning and needs assessment through the collection and analysis of data, facilitating digital payments, and enabling security in verification through digital biometric technologies' verification of aid recipients for efficiency and security.[20] The ambitions of the Grand Bargain and the nexus, particularly the transition from short-term humanitarian response to longer-term, durable solutions, have significant implications for and dependencies on the enabling digital systems, yet neither the architecture nor protection dimensions of this transition have received the necessary attention.

In this next section, we review debates on the transitioning of aid and services as part of the nexus, and review how digitalisation is transforming this transition. We outline how a particular approach to digital transformation – digital public infrastructure – might offer lessons for the humanitarian-development nexus and the transition of services and aid from short-term humanitarian response to longer-term, durable solutions, especially those provided by state actors.

Service Transition

The transfer and sharing of aid, support, and services from short-term humanitarian response to longer-term solutions, including those provided by development actors such as States, is a particularly contentious aspect of nexus

19 Shirin Madon and Emrys Schoemaker, "Digital Identity as a Platform for Improving Refugee Management," *Information Systems Journal* 31, no. 6 (2021): https://doi.org/10.1111/isj.12353.

20 Barnaby Willitts-King, John Bryant, and Kerrie Holloway, "The humanitarian 'digital divide'," *HPG Working Paper. ODI*, November 2019, https://odi.org/en/publications/the-humanitarian-digital-divide/; Pierrick Devidal, "'Back to Basics' with a Digital Twist: Humanitarian Principles and Dilemmas in the Digital Age," *Humanitarian Law & Policy Blog (blog)*, 2 February 2023, https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/.

approaches. Advocates of linking relief, rehabilitation, and development argue that they can promote sustainability, local ownership, and the progressive realisation of State responsibilities toward citizens[21] – commitments formally established in the Grand Bargain. The World Bank, for example, has explicitly framed humanitarian assistance as a building block for future State services, proposing that "components of humanitarian programming can be gradually adopted by government systems".[22]

Critics of a transfer of services highlight a number of challenges to this ambition. A fundamental challenge is the assumption that States have the willingness and capacity to provide services – an assumption that can be critiqued on both counts. In many contexts, States are party to conflict or exclude particular populations. In Yemen, for example, contested State authority over humanitarian aid relief and social protection systems has complicated the delivery of aid.[23] In these contexts, reliance on State systems may reinforce exclusion, while lack of funding and capacity can lead to the collapse of service provision.[24]

The other significant issue is that the transfer of services raises fundamental questions about humanitarian principles, with humanitarian organisations voicing concerns that alignment with States can compromise humanitarian impartiality, neutrality, and independence. *Médecins Sans Frontières*, for example, has consistently argued that the nexus risks subordinating humanitarian imperatives to ideological goals of liberal development and state-building.[25]

The transfer of data related to the transfer of services raises an existential challenge to humanitarian neutrality. As we will further discuss below, the

21 Irina Mosel and Simon Levine, "Remaking the Case for Linking Relief, Rehabilitation and Development. How LRRD Can Become a Practically Useful Concept for Assistance in Difficult Places," *ODI*, 2014, https://media.odi.org/documents/8882.pdf.

22 Ugo Gentilini, Sarah Laughton and Clare O'Brien, "Human(itarian) Capital?: Lessons on Better Connecting Humanitarian Assistance and Social Protection (English)," Social Protection and Jobs Discussion Paper, no. 1802, Washington, D.C., World Bank Group. http://documents.worldbank.org/curated/en/946401542689917993.

23 Institute of Development Studies, "Sustaining Yemeni Capacities for Social Assistance: Lessons From a Decade of War," *BASIC Research Working Paper 24*, 2024, Accessed 16 June 2025, https://www.ids.ac.uk/publications/sustaining-yemeni-capacities-for-social-assistance-lessons-from-a-decade-of-war/; Achim Wennmann and Fiona Davies. "Economic Dimensions of the Conflict in Yemen," 2020, https://repository.graduateinstitute.ch/record/299800/files/economic-dimensions-conflict-Yemen-october-2020-wennmann-davies-eu-ocha-undp.pdf.

24 Secure Livelihoods Research Consortium (SLRC), "How to support statebuilding, service delivery and recovery in fragile and conflict-affected situations," September 2017, https://securelivelihoods.org/wp-content/uploads/SLRC_briefing_29_V5_web_view.pdf.

25 Jens Pederson, "The Nexus of Peacebuilding, Development and Humanitarianism in Conflict Affected Contexts: A Respect for Boundaries," *MSF Analysis: Reflections on Humanitarian Action (blog)*, 8 January 2021, https://analysis.ocb.msf.org/nexus-peacebuilding-development-humanitarianism-conflict-affected-contexts-respect-boundaries/.

transfer of data collected for humanitarian purposes to support the provision of development support and services threatens the integrity of what is often described as humanitarian space. The transfer of data collected and processed by humanitarian organisations for humanitarian purposes to organisations for the purpose of providing aid, support, or services that are non-humanitarian in nature calls into question the exclusive purpose specification cherished by humanitarians.[26] If data collected by humanitarian organisations for the purpose of providing humanitarian support or services is used for purposes incompatible with this exclusively humanitarian purpose, including, for example, status determination, migration control, counterterrorism, etc., then humanitarian neutrality will be challenged, with highly problematic implications for the continued provision of essential humanitarian services.

Digitalisation of Services

There is a widespread, ongoing digital transformation of the systems and processes used to deliver the services that are at the core of the nexus and transition, with the turn to digital cash transfers serving as a key driver of the broader adoption of digital technologies and transformation.[27] Digital cash transfers were endorsed in the Grand Bargain[28] and have been rapidly adopted as a key element of humanitarian response, with particular support from donors who see this approach as a way of increasing efficiency and transparency in the targeting and enrolment of beneficiaries, in the delivery of assistance, and in providing choice and dignity to affected populations.[29] Digital systems and technologies, such as digital identification and beneficiary management systems such as the World Food Programme's (WFP) SCOPE platform, are able to provide the infrastructure necessary to enable a transition from humanitarian response to longer-term development efforts. Indeed, WFP has described its use of SCOPE in Chad as facilitating "interagency synergies in terms of beneficiary data and transfer management" and as "a platform that can be used to manage resilience building and social welfare initiatives in line with the Chad government's priorities".[30] Despite a number of

26 ICRC, Rules on Personal Data Protection, updated April 2025, https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

27 Madon and Schoemaker, "Digital Identity as a Platform for Improving Refugee Management".

28 'The Grand Bargain'. n.d., The CALP Network (blog), accessed 17 June 2025, https://www.calpnetwork.org/cash-and-voucher-assistance/policy-and-funding/grand-bargain/.

29 Niklas Rieger et al., "Falling Short? Humanitarian Funding and Reform," *Development Initiatives*, 2024, https://devinit.org/resources/falling-short-humanitarian-funding-reform/.

30 ReliefWeb, "SCOPE: Enabling the Change in WFP Chad (January 2019)," 27 March 2019, https://reliefweb.int/report/chad/scope-enabling-change-wfp-chad-january-2019.

humanitarian organisations – particularly WFP, the UN High Commissioner for Refugees (UNHCR), and the International Organization for Migration (IOM) – offering their platforms for State-led assistance programmes, there remains a pervasive fragmentation of digital systems across the humanitarian sector which creates a significant impediment to this potential.

Current humanitarian digital ecosystems are characterised by a proliferation of siloed management information systems, resulting in duplication of effort, inefficiencies, and inconsistent service delivery. One study of registration systems in Somalia found 13 different digital registration platforms in use by humanitarian organisations, some of which used multiple systems. It also found that organisational policies around registration result in multiple, non-interoperable data systems.[31]

There are both costs and benefits to this siloing of digital technologies and data.

The costs of humanitarian agencies having their own separate systems for registering individuals include forcing people to register multiple times with different organisations and duplicating time and effort to access services and entitlements. As a result, the digital transformation in the humanitarian sector is fragmented and siloed, with vendor lock-in and capacity constraints limiting the sector's ability to align digital transformation with its principles. These challenges are particularly driven by competing institutional interests, proprietary systems, and the absence of common standards or interoperability requirements.[32] In other words, the digital infrastructure on which an increasing amount of humanitarian response relies is characterised by fragmentation, organisational inefficiency, and even programmatic siloes that lead to a duplication of investment in systems, of individuals' time, and varying standards around data management. These problems are, however, not unique to the humanitarian sector – State service delivery has long struggled with siloes, fragmentation, and inconsistent approaches to data management.

The benefit of this siloed approach to digital systems and data processing is that the current architecture of digital infrastructure limits personal data shared by individuals to the systems and processors they have consented to share their data with, and for the purposes they have consented for their data to be used – namely for the purpose of providing humanitarian relief.

31 Boniface Owino, "Harmonising Data Systems for Cash Transfer Programming in Emergencies in Somalia," *Journal of International Humanitarian Action* 5, no. 1 (2020): 11, https://doi.org/10.1186/s41018-020-00077-1.

32 Owino, "Harmonising Data Systems".

Digital Public Infrastructure

The concept of digital public infrastructure (DPI) has emerged as a potential antidote to this fragmentation. DPI encompasses shared digital systems and standards for core services such as identification, payments, and data exchange. It is increasingly seen as a solution to capacity and cost constraints, fragmentation, and vendor lock-in – problems endemic within the humanitarian sector as well as other domains such as the public sector. Several development actors, notably the World Bank's Identification for Development (ID4D) initiative and the Gates Foundation, have embraced this approach.[33] The Digital Public Goods Alliance (DPGA) has also advanced this concept by establishing frameworks for open-source solutions that can be adapted across development contexts.[34]

A DPI approach might help the humanitarian sector to overcome these challenges. DPI reflects a shift from building specific digital systems and services to building the underlying infrastructure – that is, by way of analogy, to optimising the railway network, rather than buying expensive trains. DPI envisions digital infrastructure that is modular, so that individual components can be switched out, and interoperable, so that data can flow seamlessly between those components. A DPI approach could thus play a role in realising the policy goals of the Grand Bargain by facilitating the transition from humanitarian response to social protection, and potentially the other way around if such needs arose in a specific context.

Canonical examples of DPI are India's Aadhaar digital identification system and the 'India Stack', which has been built out from it – the first eKYC (electronic Know Your Customer) services to enable rapid identity verification, then eSign, which enables legal electronic signatures, followed by a UPI (Unified Payment Interface) that enables cashless payments, including through mobile phones, and more recently 'DigiLocker', a platform for the holding and verification of documents and certificates.[35] This collection of digital systems is owned by different ministries and crucially, in terms of enabling innovation, includes different application programming interfaces that allow businesses and others to build new applications on the data, such as

33 World Bank, Julia Clark et al., "Digital Public Infrastructure and Development: A World Bank Group Approach," *Digital Transformation White Paper*, Volume 1. Washington, DC: World Bank, http://hdl.handle.net/10986/42935; Gates Foundation, "What Is Digital Public Infrastructure?" n.d., accessed 12 June 2025, https://www.gatesfoundation.org/ideas/digital-public-infrastructure.

34 DPGA, "DPGs for DPI," https://www.digitalpublicgoods.net/collections/coll-dpi.

35 Cristian Alonso et al., "Stacking up the Benefits: Lessons from India's digital journey," *IMF Working Paper No. 23/78*, Washington D.C., 2023, https://www.imf.org/en/Publications/WP/Issues/2023/03/31/Stacking-up-the-Benefits-Lessons-from-Indias-Digital-Journey-531692.

credit rating and employee referencing. Since its establishment, the Stack has been used to enable core functionality such as personal transactions, government transfers, and services such as health and education, as well as commercial services such as insurance.

The main data governance challenges to this approach to digital transformation include concerns around privacy resulting from the collection, storage, and sharing of personal data, including sensitive biometrics, as well as risks from creating large datasets that may act as honeypots for malicious actors.

In order to assess both the potentialities for and challenges of DPI, particularly from a data protection perspective, it is helpful to review perspectives on the potential of shared infrastructure within the humanitarian sector, as well as between the humanitarian and development sectors. To do so, we draw on earlier research[36] on the feasibility of designing humanitarian aid management information systems to link with social protection systems and to support a transition – in the long term – to State-led social assistance.[37] It is also worth noting the ICRC's interest in the topic, which was one of the focal areas of its 2021 DigitHarium, i.e. digitalised assistance, social protection, and humanitarian data.[38]

Perspectives on Integrated Digital Infrastructure in Humanitarian Contexts

Opportunities for Integrated Information Infrastructure

The most common view held by professionals in the large humanitarian organisations who were interviewed[39] is that the primary value of a more integrated approach to digital infrastructure is increased effectiveness and efficiency. As one UN agency staff member noted, "where data are held in separate and fragmented MIS, there is little opportunity to use these data to recognise trends for more effective planning and response". More integrated data is

36 The original research was conducted in 2021 as part of a UK government (Department for International Development) funded effort to understand the potential for information and identification systems to link humanitarian response and State social protection. The research included a literature review and key informant interviews with a range of stakeholders at a global level as well as case studies involving local literature reviews and in-country interviews in Yemen and South Sudan. Ric Goodman et al., "Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises," *BASIC External Briefing Note*, 2020, https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/BASIC-MIS-in-Crises-2020-Final.pdf.

37 Goodman et al., "Review and Analysis of Identification and Registration Systems".

38 ICRC, "Digitalized Assistance, Social Protection and Humanitarian Data Concerns," *DigitHarium | Month #2*, 9 March 2021, https://www.icrc.org/en/digitharium/digitharium-month-2.

39 Goodman et al., "Review and Analysis of Identification and Registration Systems".

regarded as enabling better identification of patterns and needs across populations. One government donor noted that "larger datasets may also allow organisations to understand where individuals are receiving other benefits to better target or coordinate their response", potentially improving coordination and reducing gaps in assistance.

Many humanitarian professionals identified a reduced burden on beneficiaries as another significant advantage of interoperable systems, offering the potential to lessen registration fatigue for those receiving humanitarian assistance. One staff member of a large NGO noted that "data collected digitally can be immediately referenced with existing data in the information system", meaning individuals may only need to register once to access multiple services.

Others also talked about how more integrated systems within the humanitarian sector could enable easier transitions to government systems – very much in line with the promise of DPI. One technical consultant noted that "transfer to a government-led social protection system would be easiest if data are transferred from a single MIS, or from a centralised data warehouse".

Risks of Integrated Information Systems

Many humanitarian professionals interviewed also flagged the significant privacy and security concerns associated with more integrated systems and transfers of data. One humanitarian technical advisor noted that "single or centralised databases are targets for theft as they are more attractive targets due to the quantity of data". The risks of centralised datasets create additional significant protection concerns. This is particularly the case with humanitarian registration data, which contains sensitive personal information and can put already vulnerable individuals at greater risk. As one staff member from a UN humanitarian agency noted, "the value of personal data (and even more so, biometric data) for identifying individuals of concern to State, law enforcement, security and judicial bodies, is clear". The risk of transferring data collected for humanitarian purposes to States introduces new risks of data misuse by governmental authorities.[40]

More integrated systems can also lead to the combining and further analysis of what were separate datasets. Different humanitarian organisations often collect specific information for specific purposes related to their organisational mandates: UNHCR may collect personal biographic data for refugee status determination, WFP may collect family information as part of needs assessments, and the UN Children's Fund (UNICEF) may collect personal education data as part of eligibility assessment for school access. As one staff

40 Aaron Martin, "Why Sovereignty Matters for Humanitarian Data," *Big Data & Society*, 2025 (forthcoming). https://doi.org/10.1177/20539517251361109.

member of a UN agency providing services in a conflict setting noted, "where MIS share data or in the case of a single MIS with multiple users, there is a potential for mission creep, as increasing amounts of data need to be collected to satisfy different parties and their analytical and service provision needs".[41] This violates the principle of data minimisation (a key data protection concept) and increases risks to already vulnerable populations (contrary to the "do no harm" mantra of humanitarians).

Integrated systems also introduce risks around consent. Many of the humanitarian professionals interviewed highlighted that gaining informed consent was challenging due to the power asymmetries and dire need, echoing insights by other critical observers.[42] One international NGO staff member noted that "whether the responsibility to collect consent is one agency's (single system) or many, the risks with this process in the humanitarian sector are significant".[43] And most information systems do not allow individuals to exercise control or even have oversight of their data and how it is used. One interviewee noted that "many MIS do not afford individuals control over their digital identity and their own data".[44]

DPI and Personal Data Protection in Humanitarian Action

As we have argued elsewhere,[45] DPI approaches for the humanitarian sector must be framed and designed around humanitarian principles and commitments. At the core of all humanitarian actions lie the fundamental principles of humanity, impartiality, neutrality, and independence. These are codified in international humanitarian law, embraced by the United Nations through General Assembly Resolutions 46/182 and 58/114, and incorporated into sector-wide agreements such as the Core Humanitarian Standard on Quality and Accountability and SPHERE Standards.

The promotion of DPI as a contributor to Grand Bargain policy goals and broader humanitarian response requires the reframing and adaptation of DPI to meet these existing humanitarian principles and standards. This means matching the specific technical and operational dimensions of DPI – such as interoperability – against humanitarian policy commitments of protection,

41 Goodman et al., "Review and Analysis of Identification and Registration Systems".

42 Dragana Kaurin, "Data Protection and Digital Agency for Refugees," *Centre for International Governance Innovation*, 2019, https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/.

43 Goodman et al., "Review and Analysis of Identification and Registration Systems".

44 Goodman et al., "Review and Analysis of Identification and Registration Systems".

45 Rohan Pal et al., "Leveraging the DPI Approach for Multilateral Cooperation in Humanitarian Aid," *T20 Policy Brief*, 2024, https://t20brasil.org/media/documentos/arquivos/TF06_ST_01__Leveraging_the_DPI66faefb580df6.pdf.

consent, and purpose. This can be operationalised through technological design approaches such as "data protection by design" and "privacy by design",[46] and the adaptation of technical and governance dimensions of DPI to meet data protection requirements, the effective enforcement of which will be especially challenging in humanitarian settings.

While these challenges are potentially numerous and will differ according to the specificities of the technological context (digital identification, payments,[47] connectivity, etc.), here we summarise some of the most pressing considerations for humanitarian action. Others have analysed the various privacy and data protection implications of DPI,[48] which we will not rehash here. Instead, we home in on what is uniquely challenging about the potential use of DPI in humanitarian settings.

The handling of personal data by humanitarian organisations based on the promise of exclusively humanitarian use (i.e. purpose specification) is troubled in a scenario in which DPI facilitates the potential repurposing and extended uses of data, many of which may be non-humanitarian in their nature. While the sector has always struggled to ensure through legal and technical means that data collected by humanitarians is used for exclusively humanitarian purposes, the introduction of DPI could serve to make these governance problems even more complex.

Moreover, in situations in which DPI is expected to bridge humanitarian and development spaces, organisations will need to assess whether the legal basis for data processing is adequate. It might be that data collected for a humanitarian response was done so in the vital interest of the data subject. However, the use of this data for other purposes, including development aid and/or by non-humanitarian actors, could require another or an additional legal basis.

Relatedly, there is a real risk that DPI deployed in aid contexts will suffer from unmanageable function creep[49] whereby its purposes and uses expand in an uncontrolled way by dint of the interoperability made possible by the

46 Carmela Troncoso and Wouter Lueks. "Designing for Data Protection," *Handbook on Data Protection in Humanitarian Action*, Massimo Marelli ed., (Cambridge University Press, 2024) 76–95.

47 Pierrick Devidal, "Cashless Cash: Financial Inclusion or Surveillance Humanitarianism?" *Humanitarian Law & Policy Blog*, 2 March 2021, https://blogs.icrc.org/law-and-policy/2021/03/02/cashless-cash/.

48 "Digital Public Infrastructure: Policy Recommendations," 2024. *Access Now* (blog). Accessed 12 June 2025, https://www.accessnow.org/guide/digital-public-infrastructure/; Justin Sherman, "Finding Security in Digital Public Infrastructure," *Atlantic Council* (blog), 21 October 2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/finding-security-in-digital-public-infrastructure/.

49 Bert-Jaap Koops, "The Concept of Function Creep," *Law, Innovation and Technology* 13, no. 1 (2021): 29–56, https://doi.org/10.1080/17579961.2021.1898299.

underlying infrastructure. These risks are amplified by the governance challenges posed by data processing across the humanitarian, development, and peace sectors, which are often subject to different laws and regulations for data and technology, including international law, and for which oversight and enforcement may vary.

DPI and the Implications for Humanitarian Space

The implications of a DPI approach to digital transformation across the humanitarian-development nexus thus force the question of how to create and protect an exclusively humanitarian digital space.[50] The transition is not just an abstract policy consideration but also one with real implications for people. This space must balance the rights of affected populations and organisations, including preserving the ability of humanitarian actors to operate in line with their principles and squaring the organisational efficiency gains of digital transformation with the protection of humanitarian principles.

This distinction is important because the field of humanitarian action is distinct, governed by specific laws, principles, and practices. The concept of humanitarian space commonly refers to "the ability of agencies to operate freely and meet humanitarian needs in accordance with the principles of humanitarian action".[51] The question then is an enduring one, framed by Sandvik et al. as shifting from thinking about "what technology does *for* humanitarian action to asking what technology does *to* humanitarian action".[52] What then are the specific considerations that a DPI approach to digital transformation in the humanitarian sector raises, particularly in relation to its role in enabling the transition of services from humanitarian to development actors when that transition is possible or required? Secondly, what does a DPI approach do *to* humanitarian action?

In February 2025, in the midst of severe funding cuts, the UN Emergency Coordinator called for a "humanitarian reset" that would include working more closely with partners such as the World Bank and strengthening inter-agency coordination.[53] The continued commitment by the donor and humanitarian policy community to the nexus suggests a persistent view that

50 Daniel Thürer, "Dunant's Pyramid: Thoughts on the 'Humanitarian Space'," *International Review of the Red Cross* 89 no. 865 (2007): 47–61, https://international-review.icrc.org/sites/default/files/irrc-865-3.pdf.

51 Kristin Bergtora Sandvik et al., "Humanitarian Technology: A Critical Research Agenda," *International Review of the Red Cross*, 96 no. 865 (2014): 219–242, https://doi.org/10.1017/S1816383114000344.

52 Sandvik et al., "Humanitarian Technology: A Critical Research Agenda".

53 Tom Fletcher, "Humanitarian Reset," *OCHA* (blog), 20 February 2025, https://www.unocha.org/news/humanitarian-reset.

the transition of service delivery from humanitarian to local and longer-term development organisations still holds promise.[54] While there are some considerations of how a DPI approach to digitalisation in the humanitarian sector could help fulfil these goals, there are also challenges.

There are challenges when we ask what employing a DPI approach to service delivery within the context of the nexus does *to* humanitarian space. Our analysis of the digital systems that support humanitarian service delivery suggests that a DPI approach to the transitioning of services from humanitarian to development efforts may introduce significant risks to the protection of personal data, as well as a blurring of the lines between humanitarian and development spaces. While there are some technologies that may help mitigate these risks (see below), efforts to progress a more integrated approach to digitally enabled services need to take these risks into consideration when designing and delivering services.

Digital public infrastructure *within* the humanitarian sector has the potential to address some of the endemic challenges that the sector struggles with. If humanitarian organisations could use a shared system for digital identification and payments, for example, it could help reduce the cost of duplicate systems and introduce new efficiencies. This is particularly so for UN agencies, given their resources, but work by the Collaborative Cash Delivery Network (CCD)[55] and the International Federation of Red Cross and Red Crescent Societies (IFRC)[56] around data governance and interoperability indicates this has wider potential and broader appeal too. Given the continuous and increasing funding crises and proposed agenda of reform, this potential to introduce efficiencies and increase effectiveness might be a core consideration for decision makers. A more integrated approach could also introduce benefits for individuals, who would save time by only having to register once, travel less to access services, and enjoy more secure systems to store personal documents and credentials.

Yet as research with humanitarian actors shows,[57] there is significant concern about the implications of linking the different datasets and registries. Many of these concerns are based on institutional politics, whereby some actors may be loath to share data and give up the competitive advantage

54 Caitlin Sturridge and Leigh Mayhew, "Funding Cuts and Nexus Thinking: What Can Aid Actors Learn from the 'Beautiful Game'?" *ODI: Think Change* (blog), 8 May 2025, https://odi.org/en/insights/funding-cuts-nexus-thinking-humanitarian-development-peacebuilding-football/.

55 CCD, "Creating the Ecosystem, Standards, & Culture for Data Interoperability in Humanitarian Action," n.d., accessed 12 June 2025, https://www.collaborativecash.org/data-interoperability.

56 IFRC, "Interoperability," *DIGID Consortium* (blog), 29 August 2023, https://interoperability.ifrc.org/projects/interoperability/.

57 Goodman et al., "Review and Analysis of Identification and Registration Systems".

that holding large amounts of beneficiary data grants when competing for project funding.[58] There are also significant concerns about the data protection implications of linking large datasets of personal data – particularly of already vulnerable individuals.[59] Digital public infrastructure *within* the field of humanitarian response offers opportunities to make humanitarian space more integrated and, through the use of shared systems and standards, more aligned around common principles of data protection.

The role of digital public infrastructure in enabling transitions *between* the fields of humanitarian and development response presents a more complex picture. Integrated and standardised datasets and shared identification systems would enable an easier transition of social registries and data to development actors. States with established digital infrastructure, such as social registries or social protection systems, could integrate those receiving humanitarian support into existing systems. Such approaches could also lead to other benefits such as addressing legal status issues – for example, in mitigating the double registration and statelessness issue of those Kenyan nationals also registered in UNHCR databases.[60] Yet the example of double registration in Kenya also highlights the challenges of getting digitalisation right and the importance of ensuring that appropriate and adequate data protection principles and practices are upheld. There is now widespread recognition that ensuring individual agency over their personal data is a key practice that can help mitigate the unintended consequences of personal data held in humanitarian and State databases.

This challenge is only more significant when considered in the context of significant cuts to humanitarian aid and the closure of humanitarian programmes and support. As humanitarian activity retreats, there may be an expectation amongst some donors that States may take a greater role in managing the identification of and support to those who would otherwise have received humanitarian aid and services, but this assumes that these actors are interchangeable. However, there are spaces where humanitarian action is necessary because States cannot go, such as situations of conflict, and providing aid requires actors able to operate according to humanitarian principles.[61]

58 Madon and Schoemaker, "Digital Identity as a Platform for Improving Refugee Management".

59 Gianclaudio Malgieri and Jędrzej Niklas, "Vulnerable Data Subjects," *Computer Law & Security Review* 37 (2020): 105415, https://doi.org/10.1016/j.clsr.2020.105415.

60 Keren Weitzberg, "In Kenya, Thousands Left in Limbo without ID Cards," *Coda Story* (blog), 13 April 2020, https://www.codastory.com/authoritarian-tech/kenya-biometrics-double-registration/; Wangui Gitahi, "Navigating the Legal Landscape of Double Registration in Kenya," 2024. *Forced Migration Review* (blog), accessed 12 June 2025, https://www.fmreview.org/digital-disruption/gitahi/.

61 Cristina Quijano Carrasco, "Humanitarian Engagement in Social Protection: Implications for Principled Humanitarian Action," *Humanitarian Law & Policy Blog* (blog), 11 February

The transition of services and associated data will imply a transition of personal data that would be given by humanitarian organisations to States – a further blurring of the lines between humanitarian and non-humanitarian or development spaces that have already been complicated by the increased role of non-humanitarian actors, i.e. private sector and particularly tech companies. In order to ensure that humanitarian and data protection principles are upheld, this will require meaningful consent from the data subject, particularly for change of use.

DPI and the Protection of Humanitarian Space and Individuals

There is no single technology that constitutes DPI, and different technologies will afford different outcomes. In considering a DPI approach to address challenges in the humanitarian sector and between the humanitarian and development sectors, it is critical to select technologies that can best uphold humanitarian principles and thus protect humanitarian space. Defining key principles can help provide guidance to ensure that technology selection and procurement support these goals.

Design Principles and Technologies for Humanitarian DPI

Purpose limitation is the first principle that should guide a DPI approach to digital transformation in the humanitarian sector and between the humanitarian and development sectors, though as discussed above there are real tensions with limiting purposes in the expansive vision of DPI. Data minimisation follows as the second principle. By collecting only what is necessary for the humanitarian purpose, organisations can reduce risks associated with data breaches, surveillance, and mission creep. However, the principle of data minimisation may be in tension with the efficiency goals promised by more integrated and interoperable digital infrastructure, particularly when integrating the systems of humanitarian organisations with diverse goals such as collecting data for legal status determination, basic needs assessment, and medical and educational services.

Technologies that support data minimisation include systems that incorporate techniques such as zero-knowledge proofs. Zero-knowledge proofs are a cryptographic method by which one party can prove to another party that they know a value x, without conveying any information apart from the fact that they know the value.[62] For instance, Organisation A could state they have

2021, https://blogs.icrc.org/law-and-policy/2021/02/11/humanitarian-engagement-social-protection/.

62 Shafi Goldwasser, Silvio Micali, and Charles Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing* 18, no. 1 (1985): 186–208, https://doi

Beneficiary A in their system, without sharing the details of that beneficiary with Organisation B. Zero-knowledge proofs require substantial amounts of processing power – more than is available in most smartphones. This means that such proofs are better suited to institutional interactions – such as among humanitarian organisations and between humanitarian organisations and States – which will limit their immediate utility in humanitarian field action.

Privacy-by-design is an established technology design principle that has far reaching ramifications.[63] Rather than treating privacy as an afterthought, adopting privacy-by-design principles would require the selection of humanitarian digital systems that incorporate privacy protections into their core architecture. These protections include measures such as data segregation, encryption, access controls, and automatic deletion after predetermined periods.[64] Ensuring that this design principle is not lost during the transition of systems and data from humanitarian to non-humanitarian contexts is fundamental.

Privacy-by-design principles that might guide the development of digital infrastructure in the humanitarian sector could include deletion policies and processing personal data in a distributed manner, such that biographical data, biometric templates, and biometric images are always physically and logically separated from each other. Privacy-by-design also requires accountability mechanisms, and the design of digital infrastructure to enable the transition and transfer of data between humanitarian and development actors should include elements such as a tamper-proof and secure audit log of all transactions/activities to ensure user accountability and the possibility to reconstruct events and detect potential intrusions, and to identify other problems.[65]

.org/10.1137/0218012. This is the seminal paper that introduced zero-knowledge proofs. For further details: National Institute of Standards and Technology, "Privacy-Enhancing Cryptography (PEC) Zero-Knowledge Proof (ZKP)," https://csrc.nist.gov/projects/pec/zkproof.

63 Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario, Canada, 2009, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf; Jaap-Henk Hoepman, "Privacy Design Strategies (The Little Blue Book)," April 2022, https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf; GDPR (2016), particularly Article 25 on "Data protection by design and by default", which codifies privacy-by-design into law; Seda Gürses, Carmela Troncoso and Claudia Diaz, "Engineering Privacy by Design," *Computers, Privacy & Data Protection*, 2011, https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf.

64 Adamantia Rachovitsa, "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue," *International Journal of Law and Information Technology*, 24, no. 4 (2016): 374–399, https://doi.org/10.1093/ijlit/eaw012.

65 Ric Goodman et al., "Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises," *BASIC – Better Assistance in Crises. DAI and Caribou Digital*, 2020, https://reliefweb.int/report/world/basic-better-assistance-crises-review-and-analysis-identification-and-registration-0.

Federated architecture with interoperability can help maintain institutional policies and practices around data management yet enable the benefits of a more integrated approach. A federated architecture in which data ownership is maintained by each actor can maintain the independence of humanitarian actors. This approach maintains the autonomy of individual humanitarian actors while enabling controlled information sharing. The governance of interoperability mechanisms is critical, and the right technical architecture combined with detailed data sharing agreements is critical.

Conclusion

This chapter has examined how a digital public infrastructure approach to digital transformation might be part of the humanitarian sector's engagement with the transition of humanitarian aid and relief in the context of the nexus of humanitarian and development response, and increased pressures for efficiency in response to an unprecedented funding crisis. It has explored how DPI's promise of efficiencies and transformation could help respond to both challenges *within* the humanitarian sector as well as to the challenges of transition *between* the humanitarian sector and longer-term, increasingly State-led response. The chapter has reflected on how challenges of governance, namely the protection of humanitarian principles and space, are in tension with a more integrated approach to humanitarian response. However, emerging innovations, such as in privacy-enhancing technologies and privacy-by-design methodologies, could help realise the promise of digital public infrastructure and maintain the protection and principles that are only going to become more important in the face of the ever-growing need for and pressure on the provision of neutral, impartial, and independent aid and relief.

6

DATA PROTECTION AND INDEPENDENCE IN AN AGE OF HYPERCONNECTIVITY

Martin Searle

Introduction

There are worrying indications that hacking humanitarian organisations is becoming normal practice.[1] In 2022, the International Committee of the Red Cross (ICRC) was the victim of a highly sophisticated, targeted cyberattack.[2] The American, British, and Chinese governments, as well as ostensibly private groups, have reportedly used cyber-based methods to garner information from non-governmental organisations (NGOs) like *Médecins du Monde* and several United Nations (UN) agencies, including the World Health Organization.[3] Similar attacks have been documented in Syria, Greece,

1 Martin Stanley Searle, "Is Use of Cyber-Based Technology in Humanitarian Operations Leading to the Reduction of Humanitarian Independence?" *RSIS Working Paper* No. 315. Singapore, https://rsis.edu.sg/rsis-publication/nts/is-use-of-cyber-based-technology-in-humanitarian-operations-leading-to-the-reduction-of-humanitarian-independence/.

2 ICRC, "Cyber Attack on ICRC: What We Know." *International Committee of the Red Cross*, 2022, accessed 4 May 2025, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

3 Rory Byrne, "Trends in Intelligence Gathering by Governments," *Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management*, 2016, https://gisf.ngo/wp-content/uploads/2020/02/2259-EISF-2014-Trends-in-Intelligence-Gathering-by-Governments.pdf; James Ball and Nick Hopkins. "GCHQ and NSA Targeted Charities, Germans, Israeli PM, and EU Chief." *The Guardian*, 2013, https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner; Daniel Gilman, "Cyber-Warfare and Humanitarian Space," *Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management*, 2014, https://gisf.ngo/wp-content/uploads/2020/02/2250-EISF-2014-Cyber-Warfare-and-Humanitarian-Space.pdf.

DOI: 10.4324/9781003650164-10

and other places targeting NGOs, activists, civil society organisations, and people seeking aid.[4] Much of the data held by the targeted organisations is highly sensitive. It includes personal data such as names, biometric information, and identification records; health data such as medical histories; demographic data such as gender, ethnicity, and socio-economic status; financial data such as distribution records or digital transactions; and even protection data, which includes data related to potential abuse and violations of international humanitarian or human rights laws. Such hacking immediately raises concerns about the safety and dignity of the people whose data was accessed without permission. Those concerns have rightly been the focus of much of the data protection discourse in humanitarianism over the last ten years. That discourse fundamentally approaches the treatment of personal data as an extension of physical wellbeing, connecting with the humanitarian principle of humanity, especially the responsibility to "do no harm". But this chapter asks whether the appropriation of data collected by humanitarian groups – whether through hacking or through agreement with those groups – threatens another core humanitarian principle: independence. If it does, then data protection measures are necessary for the maintenance of that principle also.

The chapter begins with a review of why, in general, threats to humanitarians' independence matter. It then introduces a conceptual framework built using the notions of "digital" and "cyberspace" and operationalised using structuration theory. That framework helps account for how digital technologies, and their intimate and extensive connection through cyberspace, increase both the incentive and the opportunity for different actors to appropriate data collected by humanitarian organisations and use it for their own political, economic, and even military and security purposes. The outcome of that appropriation, the chapter argues, is the risk that independence is diminished to the point of irrelevance. Accessing data in this way is a matter of ethics, law (or its absence), and organisational policy and practice, bringing it squarely into the realm of data protection. By extension, the chapter suggests, this is where we are likely to find solutions too.

Why does Independence Matter?

Independence is often a prerequisite for a humanitarian group to negotiate access to a politically contested space.[5] To convince an authority (*de jure* or *de facto*) which could potentially block aid to instead allow it in, humanitarians

4 Byrne, "Trends in Intelligence Gathering by Governments"; Carleen Maitland and Rakesh Bharania, "Balancing Security and Other Requirements in Hastily Formed Networks: The Case of the Syrian Refugee Response," 2017, https://dx.doi.org/10.2139/ssrn.2944147.

5 Searle, "Cyber-Based Technology".

must demonstrate that they do not serve the interests of any opponent to that authority. In this sense, independence is often the tangible side of – and even a necessary condition for – neutrality. This means perceptions of independence matter as much as actual independence.

What is so convincing about independence? Here the chapter follows Antonio Donini, who connects independence to the capacity to resist "the blatant abuse and distortion of relief operations to achieve political objectives that are often antithetical to humanitarianism".[6] This includes obvious strategic and tactical military benefits and "more subtle manipulations arising from the convergence of interests... around agendas related to globalisation, peace consolidation, nation-building, human rights and justice".[7] For Ed Schenkenberg van Mierop, Executive Director of the Humanitarian Exchange and Research Centre, it entails, "being autonomous from the political, economic, military or other objectives that any actor may hold with regard to the area where humanitarian action is implemented... Independence implies institutional, political, financial and operational autonomy".[8] He goes on, quoting the Fundamental Principles of the Red Cross: "The legitimacy of any humanitarian actor stands or falls on its capacity to withstand 'any interference, whether political, ideological or economic, capable of diverting it from the course of action laid down by the requirements of humanity, impartiality and neutrality'".[9] Fundamentally, independence no longer functions to build trust and meet the requirements of these other three principles when humanitarian aid providers' agency is diminished to the point that their actions end up serving one or another non-humanitarian agenda. Most commonly, such lost agency is brought about by financial dependency. The ability and willingness of the US Bush administration to use aid groups as "force multipliers" during its regime-building efforts in Afghanistan exemplify the way such dependence can result in lost agency,[10] although this instrumentalisation of aid is often argued to be the norm rather than the exception throughout humanitarianism's history.[11] Thisconnection with legitimacy highlighted within the Red Cross Principles is particularly strong in the context of data collection. Humanitarians cannot claim to respect the dignity and agency of those about whom they produce, collect or use data if they cannot maintain

6 Antonio Donini, ed., "The Golden Fleece: Manipulation and Independence in Humanitarian Action," (Kumarian Press, 2013): 2.

7 Donini ed., "The Golden Fleece".

8 Ed Schenkenberg van Mierop, "Coming Clean on Neutrality and Independence: The Need to Assess the Application of Humanitarian Principles," *International Review of the Red Cross* 97, no. 897–898 (2015): 295–318, 299, http://dx.doi.org/10.1017/S181638311500065X.

9 Schenkenberg van Mierop, "Coming Clean on Neutrality and Independence".

10 Nematullah Bizhan. "State-Building in Afghanistan: Aid, Politics, and State Capacity," *Asian Survey* 58, no. 6 (2018): 973–994, https://www.jstor.org/stable/26606140.

11 Donini ed., "The Golden Fleece," 1–12.

control over that data and the uses to which it is put.[12] Nor can they exercise accountability to them. Yet dignity and accountability are considered core elements of the principle of humanity, which, together with impartiality, are the pre-eminent of all the humanitarian principles. Meanwhile, humanitarian groups are under significant pressure, often from donors, to share data. They work hard to find ways to satisfy this demand in ways that maintain their legitimacy.[13]

Domestic insurgencies offer excellent case studies of the practical importance of the independence principle. Demonstrating autonomy from a national government (and its various international backers) to opponents of that government is a necessary condition for establishing trust with that opposition, and *vice versa*. Again, the connection with data protection here is clear: to build trust, it is essential that any data collected does not benefit one side of the conflict or the other. Here we see the role of independence in achieving neutrality. Due in large part to its ability to demonstrate autonomy, in Afghanistan *Médecins Sans Frontières* (MSF) has been one of the only organisations able to provide tertiary level healthcare outside of Kabul both under the previous NATO-backed regime and after the return of the Taliban to power.[14] This example underscores the instrumental role of independence in achieving the other humanitarian principles: humanity and impartiality. To alleviate human suffering effectively wherever it is found (the definition of humanity), one needs the capability to reach those in need regardless of who controls the territory in which they happen to find themselves. To provide aid based on the severity of need alone (the definition of impartiality), the same is true. In humanitarianism, concepts have immediate practical application: theory is practice. Fundamentally, independence matters for its role in achieving the other core humanitarian principles of humanity, impartiality, and neutrality.

What sort of data protection is required to maintain this independence?

12 See Chapter 15, "Data sharing between humanitarian organisations and donors: accountability, transparency, and data protection in principled humanitarian action".

13 Vincent Cassard, Stuart Campo, and Jonas Belina, "Responsible data sharing between humanitarian organizations and donors: Towards a common approach," ICRC, 2023, https://blogs.icrc.org/app/uploads/sites/102/2023/06/Responsible-data-sharing-between-humanitarian-organizations.pdf.

14 Beatrice Lau and Martin Stanley Searle, "Absorbed into the war machine: what is independence when everything is connected?" *Myths and Hubris: Critical Reflections on Contemporary Humanitarian Action*. Routledge. Forthcoming.

Conceptual Framework

This chapter relies on two key concepts: digital and cyberspace. Here, digital is used in its fundamental technical definition as the representation and storage of data as binary code. This concept enables critical reflection on the increased quantity of personal data available due to digitalisation. That explosion is arguably the most significant impact digitalisation has had on the political, economic, cultural lives, and even the security of the people who are the subjects of that data. As a result, the concept of digital tends to coincide with concerns over data protection and the stakes of keeping sensitive details about individual human beings secure.[15]

The term cyberspace is defined in several ways depending on the purpose for which it is being used.[16] In this chapter, this term too is meant in its technical sense to describe the global network of interconnected information technology systems that has grown in substantial part thanks to the use of binary code for data storage and communication.[17] Fundamentally, it is the liabilities that arise from this interconnectedness between digital systems (using digital in the sense defined above), and between users of those systems, that affect independence. Other terms are in circulation, including digital space and digital infrastructure. But cyberspace seems the best choice for the purposes of this chapter because of its connotations of a single, albeit fragmented, domain. These conceptual connections prove to be helpful.

Independence, Agency, and Structure

Above, independence was defined in terms of autonomy and agency. The concept of agency – and the corollary concept of structure – both pre-date the rise of digital technology, but have nonetheless had a profound impact on its theorisation across the fields of sociology, political science, anthropology, economics, media studies, information systems, business, and others. Broadly speaking, agency refers to an agent's (either an individual or an organisation) capacity to make choices and act upon them freely. For humanitarians, this is

15 Privacy International. *Practices in the Humanitarian Sector Are Leaving Aid Recipients at Risk, PI and ICRC Find*. Privacy International, 2018, accessed 4 May 2025, https://privacyinternational.org/press-release/2510/practices-humanitarian-sector-are-leaving-aid-recipients-risk-pi-and-icrc-find.

16 Myles D. Garvey, "A Philosophical Examination on the Definition of Cyberspace," *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions*, ed. Steven Carnovale and Sengun Yeniyurt (World Scientific, 2021): 1–11; Binxing Fang, "The Definitions of Fundamental Concepts," *Cyberspace Sovereignty*, Springer, Singapore, https://lib.ugent.be/catalog/ebk01:4940000000125610.

17 National Institute of Standards and Technology (NIST). (n.d.). *Cyberspace*. NIST Computer Security Resource Center, accessed 5 June 2025, NIST Glossary.https://csrc.nist.gov/glossary/term/cyberspace

about choosing who receives support andensuring that decision is made based on need alone and not on any political or military rationale. Meanwhile, structures represent frameworks – like social institutions, norms, and systems – that function to constrain individual freedom of action. Put this way, our core enquiry is whether cyberspace is a structure, or gives rise to structures, that constrain humanitarian organisations' capacity to make choices about how to use the data they produce. In the author's view, there are three schools of thought that could be potentially relevant to this enquiry: critical realism, socio-materiality, and structuration theory.[18] Structuration theory appears to capture best the key feature of cyberspace that challenges independence: interconnectedness.

Structuration theory posits that technologies (like cyberspace) are structures. But in so doing, it holds that structures do not have a separate existence from agents. They mediate agents' interactions and behaviour, but they are also the outcome of those interactions and behaviour. This means structures are contingent on, and constantly reproduced by, human action; they have no objective existence. Therefore, structures are changed exclusively by human action. Such change is often organic and unorganised but can occur through collective mobilisation and action. Finally, in structuration theory, structures affect power, with power understood broadly as the ability to mobilise resources to achieve a desired outcome. Structures provide the rules that agents draw upon as they mobilise resources and pursue their desired outcomes.

When structuration theory is applied to data protection, it helps examine the way human behaviour and interactions produce and then conform to data protection norms on specific digital platforms. Much of this work focuses on privacy trade-offs on specific platforms and with specific firms. Companies like Google and Amazon have shaped privacy norms through their data collection policies. Users gradually conform to these norms, accepting personalised advertisements and data tracking as part of their digital experience.[19]

Structuration theory assigns significant power to agency, even as it presents agents' actions and the structures that both enable and constrain those actions as co-constitutive. This enables a more satisfactory account of

18 Two other schools are commonly mobilised to discuss the relationship between structure and agency: "Practice theory" is concerned with how *habitus* (internalised dispositions like habits and "tacit" knowledge) interacts with structured social environments. Meanwhile, "symbolic interaction" looks into agents' meaning-making processes and the influence of structures on that. We consider both unconnected to the specific issue at hand, so set them aside here.

19 Khando Khando, M. Sirajul Islam, and Shang Gao, "The Use of Structuration Theory in Empirical Information Systems Research: A Systematic Literature Review," *The Role of Digital Technologies in Shaping the Post-Pandemic World*, Savvas Papagiannidis et al., eds., Lecture Notes in Computer Science, vol. 13454 (Springer, 2022).

interconnectedness as both shaping and being shaped by the behaviour of agents, which, as we see in the following section, better captures the implications of interconnectedness on independence.

The Challenge of Interconnectedness to Humanitarian Independence

Driven by the benefits of speed, efficiency, effectiveness, and convenience, different categories of agents – including organisational ones like governments, corporations, religious groups, civil society actors, as well as private individuals – have taken more and more of their activities into cyberspace. This is well documented for humanitarians, but a few examples serve to demonstrate its extent. MSF uses telemedicine to provide medical consultations either completely remotely or to give staff by a patient's side access to specialised medical skills as required.[20] The World Food Programme (WFP) uses blockchain as part of its food aid delivery and cash transfer processes, reducing duplications, saving costs in bank fees entailed by conventional cash transfers, and enabling coordinated support across different groups using the same blockchain network.[21] The UN High Commissioner for Refugees (UNHCR) combines biometrics with blockchain technology to administer access to aid in places such as Za'atari camp in Jordan.[22] The ICRC uses AI-driven data analytics to forecast medical supply needs across its projects in Africa, the Middle East, and Europe, resulting in more efficient, cost-saving supply chain management.[23] The International Rescue Committee's (IRC) Signpost Project builds apps for refugees to download and then access critical information, organise into community groups, and engage in two-way dialogue with service providers.[24]

As a medium, cyberspace essentially remediates the relationship between different agents. Whereas those relationships used to occur exclusively in offline environments, they now occur additionally – and in many instances

20 Sophie Delaigue et al., "Seven years of telemedicine in Médecins Sans Frontières demonstrate that offering direct specialist expertise in the frontline brings clinical and educational value," *Journal of Global Health* 8, no. 2 (2018), https://doi.org/10.7189/jogh.08.020414.

21 Priscilla Boiardi and Esme Stout, "To what extent can blockchain help development co-operation actors meet the 2030 Agenda?" *OECD Development Co-operation Working Papers*, No. 95, 2021, https://doi.org/10.1787/11857cb5-en.

22 Samer Abboud, "Artificial Humanitarianism—The Data-Driven Future of Refugee Responses," Middle East Report Online, 2024, 313, https://merip.org/2025/01/artificial-humanitarianism/.

23 ETH Zurich. "AI to Support Humanitarian Action: ETH Zurich's Supply Chain Project." *Engineering Humanitarian Action*, 27 January 2025, accessed 4 May 2025, https://eha.swiss/2025/01/27/ai-to-support-humanitarian-action-eth-zurichs-supply-chain-project/.

24 John Bryant, "Digital technologies and inclusion in humanitarian response," ODI Global, 2022, https://odi.org/en/publications/digital-technologies-and-inclusion-in-humanitarian-response/.

exclusively – in online environments. Two implications connect to our discussion of independence. First, this remediation produces large amounts of data. When WFP administers refugees by requiring them to agree to digitise parts of their body, this produces data that would not otherwise exist. Every time refugees access services that require those digitised parts of their body to be scanned, this produces more data that would not otherwise exist. Second, relationships are mediated to enable interactions across time and space that are fundamentally new, unconstrained by limitations of physical distance and pre-existing social structures.[25] With such restrictions removed, the sheer number of connections has mushroomed, resulting in so-called "hyperconnectivity," in which all people and all machines that can communicate through interconnected computer networks do so.[26] Quite simply, in search of ever more speed, efficiency, effectiveness, and convenience, more substantively new connections are created between the different agents present in cyberspace. When MSF provides telemedical consultations, or IRC connects with people seeking assistance (or connects them with each other) using mobile apps, they contribute to a process in which more people use more devices connecting to more networks that come to share more common nodes and so create more pathways through which different agents can interface with each other. Humanitarian organisations, the people they help, as well as governments, rebel groups, private companies, and other individual human beings now exist in networks that connect them to each other perpetually, and through which they can potentially interface "anytime, anyplace".[27]

As an outcome of social relations, cyberspace does two notable things. First, it creates dependency. Telemedicine, and perhaps remote management models of humanitarian projects in general, exemplify this. Where a humanitarian response relies on one or other of these approaches, it simply would not be possible without the collapsing of time and space made possible through cyberspace. Second, connectivity and digitalisation become values in themselves. Sometimes this is done on the implicit assumption that they automatically improve both efficiency and effectiveness (and that such improvements are paramount). But sometimes State, business, and civil society actors simply commit to a "digital first" mentality for its own sake. Talk of connectivity as

25 Matthew R. Jones and Helena Karsten, "Giddens's Structuration Theory and Information Systems Research." *MIS Quarterly* 32, no. 1 (2008): 127–157, http://dx.doi.org/10.2307/25148831.

26 Academic Dictionaries and Encyclopedias. "Hyperconnectivity," accessed 29 April 2025, https://en-academic.com/dic.nsf/enwiki/6297355.

27 Mariek Vanden Abeele, Ralf De Wolf, and Rich Ling, "Mobile Media and Social Space: How Anytime, Anyplace Connectivity Structures Everyday Life," *Media and Communication* 6, no. 2 (2018): 5–14, https://doi.org/10.17645/mac.v6i2.1399.

a human right,[28] information as aid,[29] and even the academic discourse on "digital natives" and "digital immigrants" puts digital spaces in an almost teleological position towards which all are expected to advance.[30] Such normalisation then works to reinforce dependency and supercharge digital data production.

In the humanitarian sector, this normalisation of digitalisation and connectivity has been especially prominent in critical reflection about the disruption of pre-existing data management practices. Academics highlight changes in assumptions about who owns data and the weakened ability of data subjects to maintain control over their data.[31] The cyberspace concept helps deepen these enquiries to consider risks of unauthorised access, alteration, or deletion, and subsequent issues of data governance,[32] all centred on the risks posed to the wellbeing of data subjects. But that same personal data about specific individuals (their location, identity markers, socio-demographic information) could also have political, economic, or even military relevance to some actors. This further connects the question of who gains access to that data – whether through agreement based on data management norms or through hacking – to independence as defined above.

Here our concerns over data subjects' wellbeing and independence regard substantively the same data. So, by extension, data protection-strengthening measures such as unambiguous, legitimate, and rigid purpose specification; data minimisation in accordance with that specified purpose; data destruction; and improvements to overall cybersecurity through technical and regulatory means should already help strengthen independence. But also, existing challenges to protecting data that threatens wellbeing will also undermine

28 Nicholas Negroponte, "Connectivity as a Human Right," *Berkeley Center for New Media Art, Technology, and Culture Colloquium*, 2018, accessed 4 May 2025, https://archive.org/details/201825NicholasNegroponte.

29 See Chapter 2, "From Disconnected to Connected: How 10 Years of Increasing Connectivity for Crisis-Affected Communities has Heightened Providers' Responsibility to Protect Personal Data Conduits".

30 Karlie M. Mirabelli and Brandon K. Schultz, "Digital Native," *Encyclopedia of Behavioral Medicine*, Marc D. Gellman ed. (Springer, 2020), https://doi.org/10.1007/978-3-030-39903-0_101949.

31 Centre for Humanitarian Action. *Data & Digitalisation: Enhancing Digital Literacy in Humanitarian Action*, 2023, accessed 4 May 2025, https://www.chaberlin.org/en/topics/data-digitalisation/; Giulio Coppi, "Mapping Humanitarian Tech: Exposing Protection Gaps in Digital Transformation Programmes," *Access Now*, 2024, accessed 4 May 2025, https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf.

32 Dimitrios Sargiotis, "Data Security and Privacy: Protecting Sensitive Information," *Data Governance*, (Springer, 2024), https://doi.org/10.1007/978-3-031-67268-2_6; Massimo Marelli ed., ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition, Cambridge, 2024, https://doi.org/10.1017/9781009414630.

independence. As raised elsewhere in this volume,[33] use of third-party service providers is a particular concern here. These third parties are often bound by law to hand over data to authorities overseeing the jurisdictions in which they operate in certain circumstances, for example when that data is deemed relevant to national security. If those third-party providers are supporting humanitarians to manage their data, then that data too is subject to the same contingencies. Humanitarians would then very quickly become connected to those same national security agendas.

Compounding this threat to independence, captured within existing data protection concerns, humanitarians' norm conformity has also led to the production of data not covered by existing discussions of data protection. For instance, several forms of connectivity and digitalisation result in humanitarians producing more data about their own processes. Internet of Things technology has been used for a range of such purposes, including supply chain management[34] and cold chain maintenance.[35] Similarly, several context-monitoring techniques, including digital epidemiological surveillance,[36] or social network analysis,[37] produce significant amounts of digital data that is unlikely to raise protection concerns as they do not have obvious implications for any data subject's wellbeing. But that data could also help other actors further their various agendas if they can gain access to it, perhaps through mutual agreement, direct pressure, or, failing that, without authorisation.

Meanwhile, these same structures make such unauthorised access easier. The remediation of relationships by expressing them as data and the subsequent mushrooming of data quantities; reduced restrictions of space, time, and pre-existing social structures; the growth in substantive connections between agents and subsequent dependency on digital technology – all come together to create what Jacquelyn Schneider first termed as a "capability-vulnerability"

33 See Chapter 1, "The Contribution of Data Protection to Humanitarian Action: Ten Years of Data Protection in Humanitarian Action", and Chapter 5, "Digital Transformation and the Humanitarian-Development Transition: The Role of Digital Public Infrastructure and Data Protection".

34 Frontier Tech Hub, "Smart GeoSeals pilot report: Using technology to improve humanitarian supply chains," 2024, https://www.frontiertechhub.org/insights/geoseals-pilot-report.

35 Alex Fabiano Garcia and Wanderley Lopes de Souza, "Internet of Things Applications for Cold Chain Vaccine Tracking: A Systematic Literature Review," *ITNG 2023 20th International Conference on Information Technology-New Generations*, Shahram Latifi, ed., Advances in Intelligent Systems and Computing, vol. 1445. Springer, Cham, https://doi.org/10.1007/978-3-031-28332-1_37.

36 Sirwan Khalid Ahmed et al., "The role of digital health in revolutionizing healthcare delivery and improving health outcomes in conflict zones," *Digit Health* 9 (2023), https://doi.org/10.1177/20552076231218158.

37 Romina Cachia and Daniel Holgado Ramos, "Network analysis as a tool for humanitarian protection: research and practice," *Int J Humanitarian Action* 5, no. 5 (2020): https://doi.org/10.1186/s41018-020-00071-7.

paradox.[38] Following Schneider, as organisations connect more of their functions to cyberspace, they increase the so-called attack surface available for any other entity willing to penetrate that organisation.[39] Military examples illustrate this paradox best. Connecting weapons systems with each other through cyberspace enables coordination between component parts that results in exponential increases in lethality. But that same means of dramatically increasing effectiveness also provides a new means through which the entire system can be compromised. The more connections a system has, the more entry points there are for an outsider seeking to access it.

Two digital trends suggest some actors may have strong incentives to exploit humanitarians' vulnerability here. First, in parallel to humanitarians producing more data as part of their work, actors operating in the same environment are developing more ways to use data as they pursue their own agendas. Surveillance exemplifies this. The disproportionate State use of monitoring technologies on marginalised groups – who are also most likely to receive support from humanitarian groups – is well documented.[40] Similarly, surveillance capitalism often disproportionately targets marginalised groups due at least in part to the lower protections given against exploitation and the drive for market expansion.[41] This trend is exacerbated by the limited resources humanitarian organisations have to put towards cybersecurity and the inherent instability of internet connectivity in unstable or low-resource settings, which presents a significant technical barrier to arranging serious cybersecurity even

38 Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War." *Journal of Strategic Studies* 42, no. 6 (2019): 841–863, https://doi.org/10.1080/01402390.2019.1627209; Martin Stanley Searle, "Is Use of Cyber-Based Technology in Humanitarian Operations Leading to the Reduction of Humanitarian Independence?" S. Rajaratnam School of International Studies, Nanyang Technological University, 2018, https://dr.ntu.edu.sg/bitstream/10356/89619/2/WP315.pdf.

39 Massimo Marelli, "The SolarWinds Hack: Lessons for International Humanitarian Organizations." *International Review of the Red Cross* 104, no. 919 (2022): 1267–1284, https://doi.org/10.1017/S1816383122000194.

40 Evani Radiya-Dixit and Nina Toft Djanegara, "Race and Surveillance Brief," Center for Comparative Studies in Race & Ethnicity, Stanford University, 2023, https://ccsre.stanford.edu/projects/race-and-surveillance-brief; Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *NYU Review of Law and Social Change* 42, no. 2 (2018): 253–308, https://scholarship.law.wm.edu/facpubs/1883; Claudia Aradau and Emma McCluskey, "Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes," *International Political Sociology* 16, no. 1 (2022), https://doi.org/10.1093/ips/olab024.

41 Yahya Alshamy et al., "Surveillance Capitalism and the Surveillance State: A Comparative Institutional Analysis." *Constitutional Political Economy* (2024), https://doi.org/10.1007/s10602-024-09438-z; Josh Lauer and Kenneth Lipartito, *Surveillance Capitalism in America*. Philadelphia: University of Pennsylvania Press, 2021.

if resources are invested to do so.[42] This is further compounded by an overall lack of digital literacy.

The second trend is the so-called "death of causality" in statistical analysis.[43] This refers to the tendency for Big Data models to sideline concerns about causal mechanisms in establishing the existence of relationships between variables. Big Data methods purport to have made such concerns obsolete. Where data was once collected to test a specific hypothesis – with the result that data collection was directed and intentional – now data is harvested *en masse* and parsed for correlation-based insights. When it is a matter of finding correlations, improving AI performance, and helping neural networks generalise better, the more data, the better. There is significant discussion of these approaches in predictive policing[44] and healthcare diagnostics,[45] both of which could motivate interest in data collected by humanitarians due to the securitisation of minority and marginalised populations and the inherent focus on healthcare in humanitarian work.

Of greatest alarm, combining both the trends of increased surveillance enabled by digital technology and the death of causality, militaries are applying such correlation-driven methods to identify targets to attack. Israel's Gospel System does this by rapidly analysing vast quantities of surveillance data to recommend targets.[46] It does this based on presumed probability that proposed targets are individual enemy combatants, private homes of such combatants, or command posts. The US has been accused of using similar methods to

42 Budi Dhaju Parmadi and Kalamullah Ramli, "Transforming humanitarian response with IoT in conflict zones: Field insights, ethical frameworks, and deployment challenges," *International Journal of Electrical, Computer and Biomedical Engineering* 3, no. 1 (2025): 157–187, https://doi.org/10.62146/ijecbe.v3i1.112.

43 Jordi Vallverdú, "The Birth of Multicausality as the Death of Causality and Their Statistical Corollaries," in *Bayesians Versus Frequentists, A Philosophical Debate on Statistical Reasoning*, 77–91. Cham: Springer, 2015, https://doi.org/10.1007/978-3-662-48638-2_6; Hossein Hassani, Xu Huang, and Mansi Ghodsi, "Big Data and Causality," *Annals of Data Science* 5, no. 1 (2017): 133–156. Cham: Springer, https://link.springer.com/article/10.1007/s40745-017-0122-3.

44 Mareile Kaufmann, Simon Egbert and Matthias Leese, "Predictive Policing and the Politics of Patterns," *British Journal of Criminology* 59, no. 3 (2019): 674–693. https://www.jstor.org/stable/26780929; Gstrein, Oskar Joseph., Bunnik, Anna, & Zwitter, Andrej. Ethical, legal and social challenges of Predictive Policing. *Católica Law Review* 3, no. 3 (2019): 77–98.

45 Shirui Yu et al., "A Study on Large-Scale Disease Causality Discovery from Biomedical Literature," *BMC Medical Informatics and Decision Making* 25, no. 1 (2025): Article 136, https://doi.org/10.1186/s12911-025-02893-0.

46 Jonathan Fenton-Harvey, "The Gospel: Israel's Controversial AI Used in the Gaza War," *The New Arab*, 2023, accessed 4 May 2025, https://www.newarab.com/analysis/gospel-israels-controversial-ai-used-gaza-war.

compile "kill lists" of suspected terrorists.[47] By definition, humanitarians are often collecting and producing data in conflict settings and other places where target identification is occurring. Indeed, they are arguably producing evermore data about such contexts, some falling within the perimeter of existing concerns about data protection, some not. It is certainly conceivable, perhaps even likely, that correlations will be tested and even confirmed to exist among that growing pool of data that helps with such target identification. That data may already be produced with the help of third-party service providers who themselves have enormous contracts with governments and their militaries, making this sort of independence-sapping exploratory testing extremely easy to do.[48] Even if there is no such third-party support, the motives to hack humanitarians to access that data are plain and, as mentioned at the start of this chapter, already apparently normalised.

Conclusion and Recommendations

Fundamentally, structuration theory shows humanitarians' increasing penetration in cyberspace to be an exercise in binding themselves to a structure that is at best agnostic about their independence – in the sense that anyone acting in ways that erode that independence is left alone to do so – and at worst antithetical to it – in the sense that anyone acting in ways that erode decision-making autonomy is helped to do so by norms and principles that cyberspace has produced.

Digital technology is mediating social relations in a way that produces a far greater quantity of data than those relations produced in the past. Much of that data has the potential to help non-humanitarian political, military, or economic agendas. Where digital technologies come together to create cyberspace, structuration theory suggests they are mediating relations in ways that spawn enormous numbers of pathways through which different agents can interface with each other. Humanitarian groups – one subset of these agents – now exist in networks that connect them perpetually to those who might use the data they produce for these same political, military, or economic agendas.

As an outcome of social relations, structuration theory shows how this mediation has bound humanitarian work to relentless data production

47 Britain Eakin, "Targeted for Death, Journalists Take U.S. to Court on Kill List," *Courthouse News Service*, 2017, accessed 4 May 2025, https://www.courthousenews.com/targeted-death-journalists-take-u-s-kill-list-court/.

48 Kanishka Singh, "OpenAI wins $200 million US defense contract," *Reuters*, 16 June 2025, https://www.reuters.com/world/us/openai-wins-200-million-us-defense-contract-2025-06-16/; Jen Judson, "Tech execs enlist in Army Reserve for new innovation detachment," *Defense News*, 13 June 2025, https://www.defensenews.com/land/2025/06/13/tech-execs-enlist-in-army-reserve-for-new-innovation-detachment/.

structures. The theory crystallises the subsequent shift in mindset to normalise the idea that anything that can be done online should be done online. Donors, governments, and people receiving aid all expect aid programmes to be delivered through online means that have been optimised by cogent use of available computational power. When combined with demands for speed, efficiency, effectiveness, and convenience, the pressure for humanitarian groups to leverage cyberspace as much as they can – and to further increase the number of "anytime, anyhow" connections through which others can potentially interface with them – is enormous.

That increase in perpetual connections expands the attack surface available in cyberspace for any actor to target humanitarian groups, penetrate their systems, access the growing quantity of data they have stored, and take actions based on it. Returning to our initial definition of humanitarian independence provided by Donini, such appropriation – whether by agreement or surreptitious access – constitutes a failure to resist "the blatant abuse and distortion of relief operations to achieve political objectives that are often antithetical to humanitarianism".[49] Such appropriation, when it happens, is a violation of data protection.

This use of structuration theory suggests the threat to humanitarians' independence stems from three sources: digitalisation (i.e. the swelling of digital data production), cyberspace (i.e. the sheer number of perpetual connections that exist between humanitarian organisations and others), and the erosion of norms governing the behaviour of those others towards humanitarian organisations. Addressing these three sources entails steps that exist to some extent already in data protection literature.

First, humanitarians should review the extent to which they digitise in the sense of producing and storing data in binary code. This already conforms with best data hygiene practices of data minimisation exemplified by the ICRC's most recent handbook on this issue.[50] However, current practice focuses predominantly on data that could affect the wellbeing of data subjects if control of it were lost. To help preserve independence, these best practices should be applied to other data that does not have any immediate connection to wellbeing, but could nonetheless connect and support political, military, or economic agendas from which humanitarians must keep their distance if they are to maintain trust and remain operational. In practice, this may be as simple as extending the scope of Data Protection Impact Assessments so that they consider these other types of data in addition to the existing focus on personal or sensitive data. We might also extend the general caution that

49 Donini ed., "The Golden Fleece".
50 Marelli, *Handbook on Data Protection in Humanitarian Action*.

is advised towards data handling to cover a wider range of data types beyond just those that could impact the wellbeing of data subjects.

Second, humanitarians should reduce the number of connections between machines on their own networks and the internet. This again aligns with existing data protection thinking, where there is recognition that the attack surface offered by a large volume of connections erodes the ability to protect data.[51] The independence-oriented lens used in this chapter adds to this call by bringing the strength of hostile actors' motivations to exploit that weakness into sharper focus. The capabilities those actors hope to develop through gathering and analysing data – whether in terms of profits, military gain, or political power – are enormous. Meanwhile, the methods involved are hungry, necessitating the gathering of vast swathes of data that extend well beyond the bounds of personal or sensitive data alone.

Taken together, these first two approaches imply a level of strategic disconnection is necessary and a return to analogue methods in some circumstances, in much the same way as the debate in the military context has gone.[52] This would involve pushing back against "digital first" norms centred on efficiency, effectiveness, and convenience – a tall order in a world of shrinking humanitarian budgets and heightened efforts by States both sending and receiving aid to increase their control over it. Such pushback, in turn, will require working with donors and with recipient governments to review how the important role they both play in terms of accountability as well as service provision and sustainability must be balanced not only by concerns of privacy, dignity and humanity, but also the separation of humanitarian purposes from any other political or economic agenda

Third, humanitarians must work to "re-embed" the notion of humanitarian independence as a norm to govern the behaviour of actors in cyberspace just as it does in physical space. Once more, this is in line with existing data protection work. Here, the past ten years of experience have fundamentally been an analogous exercise in reintroducing norms into cyberspace related to doing no harm that already existed in the physical world. Work around digital sovereignty and data sovereignty exemplify this.[53] In foregrounding the actions of agents in the (re)creation of structure, structuration theory suggests further that the reintroduction of independence as a norm must be tailored differently for the different agents whose behaviour is eroding it.

For States, the approach may well be via domestic and/or international law, including International Humanitarian Law (IHL). Here, a vigorous debate

51 Marelli, "The SolarWinds Hack".

52 Jonathan Panter, "Now Hear This: The Navy Is Unprepared for Analog War." *Proceedings* 144, no. 4 (2018): 1382. U.S. Naval Institute, https://www.usni.org/magazines/proceedings/2018/april/now-hear-navy-unprepared-analog-war.

53 Marelli, "The SolarWinds Hack".

already exists on the applicability and legal and practical limitations of current law and the subsequent need or desirability for new law.[54] IHL-based approaches alone are unlikely to be sufficient for States. For non-state belligerents, the legal options may be even more limited, although IHL may still offer some possibilities. In addition, we foresee a need for direct, bilateral engagement similar to negotiations that are already done to maintain "humanitarian space" in which to operate. These need to extend into the cyberspace. Private companies and individuals may well only be bound by domestic laws and norms, although again bilateral campaigns appealing to social responsibility could prove a fruitful line of engagement.

The direction suggested by this use of structuration theory is, in many ways, an extension of the past ten years of data protection work in the humanitarian space. The progress made there gives hope. And the stakes are high: a loss of independence, and the trust it brings among those with the power to grant and block access, threatens the very legitimacy of humanitarian work.

54 Lau and Searle, "Absorbed into the war machine".

7

DATA PROTECTION AS A FOUNDATIONAL PILLAR AND KEY ENABLER OF TRUSTED DIGITAL TRANSFORMATION

Charlotte Lindsey Curtet[1]

Introduction

Data protection and digital transformation became a focus for some humanitarian organisations over a decade ago, driven by changes in connectivity, the emergence of new technologies, and evolving regulatory landscapes. However, this shift was not simply about adopting new tools. Information and Communication Technologies (ICT) began to directly shape humanitarian response efforts and enabled the collection and analysis of growing volumes of data, particularly personal information about individuals. This evolution raised significant challenges: the potential for technological intrusion, complex regulatory and ethical implications, and heightened risks for both humanitarian organisations and the people they serve.

This chapter explores the integration of data protection at the International Committee of the Red Cross (ICRC) – initially as an enabler for the Restoring Family Links (RFL) programme, and later as a foundational element of the organisation's digital transformation. It examines the contextual factors that

1 The author was the ICRC's Director of Digital Transformation and Data (2018–2020) and Director of Communication and Information Management (2010–2018), overseeing ICT, Archives and Information Management, the Data Protection Office, and Public and Corporate Communication. She was responsible for the development of the Strategy for Information Management, Systems and Technology v.1 (2012–2017) and v.2 (Digital Transformation Strategy, 2018–2025), supporting documents, and implementation plans. She also initiated the conceptualisation of the ICRC's secure digital platform (later developed as RedSafe – see Chapter 3, "The challenges of building RedSafe, a secure digital humanitarian platform: An unsafe journey?"). The opinions and views expressed in this chapter are the author's own and do not necessarily represent those of the ICRC.

DOI: 10.4324/9781003650164-11

shaped the development and implementation of data protection and digitalisation at the ICRC during the period 2010–2020. Emphasis is placed on the impact on trust, the responsibility to "do no harm",[2] and the difficult trade-offs the ICRC faced.

The ICRC's Data Protection Approach: An Enabler of the Restoring Family Links programme

The ICRC had long regarded the confidentiality of an individual's personal data as inherent and critical to fulfilling its mandate, and over time this commitment had evolved to encompass a broader recognition of an individual's agency and accountability in data use, which was reflected in key documents, though not yet systematically or digitally adapted. From 2002, it developed, in relation to missing persons, "general principles regarding the legal protection of personal data and the identification of persons unaccounted for which could be upheld worldwide, … in order to ensure best practices from all those involved in resolving issues related to missing persons".[3] In its 2008 Protection Policy, there is a mention of "protection of personal data" as part of the ICRC's methodological approach and working procedures, and more extensively in its 2009 Protection Standards as protection of "sensitive information".[4] The ICRC Assistance Policy 2004 had a reference to "protected data" with regard

2 Mary B. Anderson, *Do No Harm: How Aid Can Support Peace—or War* (Lynne Rienner Publishers, 1999). The "Do No Harm" principle in humanitarian aid emphasises that interventions should avoid causing unintended negative consequences, such as exacerbating conflicts or creating dependencies. Anderson highlighted how well-intentioned aid could inadvertently fuel tensions if not carefully implemented.

3 ICRC *The Missing: The Legal Protection of Personal Data & Human Remains*, ICRC electronic workshop, Final report and outcome, included in the preparatory documents for the 2003 International Conference of governmental and non-governmental Experts on the missing, 2002, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_themissing_072002_en_1.pdf.

4 ICRC, ICRC Protection Policy (as published in the International Review of the Red Cross, 2008), 773, https://international-review.icrc.org/articles/icrc-protection-policy. In these Standards, protection of sensitive information was extensively addressed, however, data protection was only referenced in one of the Standards: "Protection actors must collect and handle information containing personal details in accordance with the rules and principles of IHL, IHRL, and relevant national laws on individual data protection" 59. These Standards are now in their 4th edition, https://globalprotectioncluster.org/sites/default/files/2022-09/b0687fcbbbd8e82e852576810057e6be-icrc-protectionstandards-nov2009.pdf.

to data sharing.[5] The Health Division also had practices around the protection of medical data.[6]

The ICRC did not have a specific, comprehensive data protection approach. This changed in response to evolutions in the ICRC's operating environment – particularly the European Commission's announcement in November 2010 of plans to reform the European Union's (EU) data protection framework to strengthen individuals' rights, partly due to concerns about the misuse of personal data.[7] Similar initiatives were emerging across the world, for example, in Brazil,[8] Kenya,[9] and Nigeria.[10]

The ICRC recognised[11] the risks for its RFL programme,[12] which seeks to reconnect family members separated by conflict, disaster, or migration, and to help clarify the fate of missing persons. Run in cooperation with National Red Cross and Red Crescent Societies, the programme necessitates the cross-border transfer of personal data and the receipt of data from entities subject to national data protection laws.

The ICRC sought to both understand the potential implications of the evolving data protection landscape and assess its response. By January 2012, the European Commission had already proposed the General Data Protection Regulation (GDPR), which was adopted in April 2016. Although the ICRC is not subject to the GDPR – as an international organisation with privileges

5 ICRC, 2004 ICRC Assistance Policy (public version), https://library.icrc.org/library/docs/DOC/irrc-855-policy-assistance.pdf. See 6.2.4 Assessment reports: "These must contain timely, concise information that facilitates the planning and implementation of appropriate responses to needs. … Information on health, water, sanitation and economic security may be shared with the other humanitarian organizations involved and with the authorities concerned, except for data relating to security and politically sensitive or protected data", 692.

6 ICRC, Health Strategy 2014–2018, as referred to in the introduction of the Health Strategy 2020–2023, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-4203.pdf.

7 European Commission, *A Comprehensive Approach on Personal Data Protection in the European Union*, COM(2010) 609 final, 4 November 2010, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0609.

8 CMS Legal Services EEIG, *Data Protection Laws of the World: Brazil*, accessed 25 April 2025, https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/brazil.

9 Kenya, *The Data Protection Act, No. 24 of 2019*, Kenya Gazette Supplement No. 181 (Acts No. 24), 11 November 2019, https://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

10 National Information Technology Development Agency (NITDA), *Nigeria Data Protection Regulation 2019*, issued 25 January 2019, https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf.

11 Discussion between the Head of the ICRC's Protection Division and the author when she was the Director of the newly created Department of Communication and Information Management, 2010.

12 ICRC, *Reconnecting families: Preventing separation, searching for the missing, reuniting loved ones*, https://www.icrc.org/en/what-we-do/reconnecting-families.

and immunities,[13] a mandate under international law, and headquartered in Switzerland, which is not an EU member state – it does process sensitive data from entities within EU member states that are bound by the Regulation. The ICRC prioritised a focus on formulations of GDPR provisions compatible with the specificities of humanitarian action,[14] based on the need to safeguard the confidentiality of its work and to receive data based on important grounds of public interest.[15]

Defining the ICRC's Data Protection Approach and for RFL

The ICRC convened a series of meetings from 2013 to 2015 with National Red Cross and Red Crescent Societies and the International Federation of Red Cross and Red Crescent Societies (IFRC). These discussions culminated in the adoption of the Restoring Family Links Code of Conduct on Data Protection in 2015,[16] with an endorsement from the Council of Delegates.[17] The Code aimed to ensure the protection of the rights and freedoms of individuals involved in RFL activities – particularly their right to privacy and the protection of their personal data. It acknowledged the necessity of this protection due to the transfer of personal data within the Movement and to other entities, as well as the evolving regulatory landscape concerning data

13 International organisations enjoy privileges and immunities, in particular to ensure that they can perform the mandate attributed to them by the international community under international law in full independence, and are not covered by the jurisdiction of the countries in which they work. Massimo Marelli ed., ICRC, Handbook on Data Protection in Humanitarian Action, 3rd edition, Cambridge, 2024, https://doi.org/10.1017/9781009414630.

14 Through a Data Protection Project set up by the then-Director, the author of this chapter.

15 The GDPR was adopted by the European Parliament and the Council of the European Union in April 2016 and became enforceable in May 2018. Article 49 of the GDPR includes specific derogations that permit the transfer of personal data under certain conditions, such as for important reasons of public interest or to protect the vital interests of individuals. European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Official Journal of the European Union L 119, 4 May, 2016, 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

16 ICRC, Restoring Family Links code of conduct on data protection, 27 January 2016, https://www.icrc.org/en/document/rfl-code-conduct.

17 The International Red Cross and Red Crescent Movement comprises three components: the ICRC, IFRC, and 191 National Societies. The Statutory Meetings of the Movement are the highest-level forums for decision-making, coordination, and cooperation: the Council of Delegates – bringing together the ICRC, IFRC, and National Societies – and the International Conference, which convenes these three components alongside States party to the Geneva Conventions.

protection laws and standards. Following its adoption, data protection was incorporated into the new RFL Strategy.[18]

The ICRC developed its data protection capabilities in parallel to evolving regulatory requirements and with a commitment to align with international standards without being subject to them. This led to the specific inclusion of data protection in the ICRC's 2015–2018 Institutional Strategy[19] which set the objective to: "Influence and ensure compliance with emerging data protection regulatory developments, given their direct or potential impact on the ICRC's continued ability to fulfil its mandate and to carry out its humanitarian activities".[20]

This inclusion marked a significant step in recognising data protection as integral to humanitarian action. It highlighted the ICRC's commitment to safeguarding individuals' rights and ensuring the continuity of operations. The speed with which its approach was developed underscored the urgency. By 2015, the ICRC adopted its Rules on Personal Data Protection,[21] a comprehensive framework to safeguard personal data across all activities. That same year, it established its Data Protection Office[22] and Data Protection Commission,[23] the latter to ensure that the ICRC's processing of personal data adheres to internal standards and to address possible complaints from individuals – primarily beneficiaries but also including staff members – regarding the handling of their personal data.

18 Restoring Family Links Strategy for the International Red Cross and Red Crescent Movement (2008–2018), adopted by Resolution 4 of the Council of Delegates, November 2007 (Geneva: ICRC, 2008), https://www.icrc.org/en/publication/0967-restoring-family-links-strategy. Restoring Family Links: Strategy for the International Red Cross and Red Crescent Movement 2020–2025 – Including Legal References, adopted by Resolution 6 of the 2019 Council of Delegates (Geneva: ICRC, 2019), https://www.icrc.org/en/publication/4507-restoring-family-links-strategy-international-red-cross-and-red-crescent-movement.

19 The ICRC Institutional Strategy is the roadmap that guides its humanitarian efforts and objectives, https://www.icrc.org/en/our-strategies-policies-and-code-conduct.

20 ICRC Strategy 2015–2018, adopted by the ICRC Assembly on 18 June 2014 (Geneva: ICRC, 2014), 13, https://www.icrc.org/en/publication/4203-icrc-strategy-2015-2018-adopted-icrc-assembly-18-june-2014.

As Director, the author contributed to developing the Institutional Strategy and led the formulation of the second Strategy for Information Management, Systems, and Technology, on digital transformation.

21 ICRC Rules on Personal Data Protection, adopted 24 February 2015, revised 10 November 2015, and updated in 2019, 2020, and 2025, https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

22 Originally with two staff, and gradually expanding over subsequent years, the team peaked at 18 staff in 2022, before stabilising at a smaller size thereafter.

23 The ICRC Data Protection Commission, 27 January 2016, https://www.icrc.org/en/document/icrc-data-protection-independent-control-commission.

The approach aligned with the ICRC's protection approach – which recognises that protecting personal data is part of protecting a person's life, safety, and dignity – and maintains the organisation's independence. This required that the ICRC was not subject to the authority of other entities and preserved its ability to act in favour of people affected by armed conflict and other situations of violence.

Risk Landscape as Backdrop for the ICRC's Digital Transformation

The ICRC developed its first Information Environment Strategy: Information Management, Systems and Technology (2012–2017), which focused on optimising its performance by upgrading its ICT infrastructure and information management capacities. It did not include any focus on data protection. This changed as the evolving regulatory landscape was heading towards a strengthening of data protection regulation as a tool to address the growing concerns over risks deriving from digitalisation.

The ICRC was also trying to understand the risks associated with data access – risks shaped by technical systems, legal frameworks, and policy. These concerns are reflected in the ICRC's research, reports, and initiatives during this period, which addressed risks and themes such as the use of messaging apps,[24] metadata,[25] digital risks,[26] biometrics,[27] digital emblems,[28]

24 ICRC, The Engine Room and Block Party, Humanitarian Futures for Messaging Apps, January 2017, https://www.icrc.org/sites/default/files/document/file_list/humanitarian-futures-for-messaging-apps.pdf.

25 ICRC and Privacy International, "The Humanitarian Metadata Problem; 'Doing No Harm' in the Digital Era," October 2018, https://www.icrc.org/sites/default/files/document/file_list/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

26 ICRC, Symposium Report: Digital Risks in Armed Conflicts, December 2018 (Geneva: ICRC, 2019), https://www.icrc.org/en/publication/4403-symposium-report-digital-risks-armed-conflicts.

27 Biometric data is personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, which allows or confirms the unique identification of that person. ICRC, Facilitating innovation, ensuring protection: the ICRC Biometrics Policy, Humanitarian Law and Policy Blog, 2019, https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.

28 ICRC, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions (Geneva: ICRC, 2022), https://www.icrc.org/en/document/icrc-digital-emblems-report.

surveillance,[29] spyware,[30] norms on responsible behaviour in the use of ICT,[31] and laws enabling government access to data in cloud.[32]

The 2018 ICRC Digital Risk Symposium united some 170 experts from international and non-governmental organisations, academia, governments, and the tech sector. It focused on understanding how specific technological characteristics and capabilities cause harm in armed conflict situations. The Symposium Report emphasised the importance of due diligence before adopting new technologies to assess risks to individuals and the potential impact on privacy and system security, thereby enabling mitigating actions. Recommendations on data protection advocated for the integration of established practices, including data minimisation, data protection impact assessments, data protection by design, and upholding data subjects' rights in humanitarian operations.[33]

The Symposium and Report also revisited the responsibility to "do no harm", urging the humanitarian sector to reevaluate its application in the digital age. This, it stated, should involve assessing the risks associated with digital technologies, exploring responsible mitigation strategies, defining necessary accountability mechanisms, and preparing for potential remedial actions should issues arise.[34]

Addressing many of these risks and mitigations, the ICRC's first Handbook on Data Protection in Humanitarian Action was published in 2017.[35] Developed in collaboration with experts and academic institutions, it provides practical guidance on applying data protection principles in humanitarian contexts.

29 ICRC, Symposium Report: Digital Risks in Armed Conflicts, December 2018.

30 Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender," Citizen Lab, 24 August 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/. See also ICRC, Symposium Report: Digital Risks in Armed Conflicts.

31 The UN General Assembly created two parallel processes: the Group of Governmental Experts (GGE, a small expert group) on Developments in the Field of Information and Telecommunications in the Context of International Security; and the Open-Ended Working Group (OEWG, open to all States) on developments in the field of information and telecommunications in the context of international security. Between 2015 and 2018, UN efforts to promote responsible State behaviour in the use of ICT were marked by the establishment of 11 voluntary, non-binding norms and subsequent challenges in achieving consensus on their application and over the applicability of international law to cyberspace.

32 See ICRC Handbook on Data Protection, Chapter 11.

33 ICRC, Symposium Report, Digital Risks in Armed Conflict, 4, 19.

34 ICRC, Symposium Report: Digital Risks in Armed Conflicts, 18.

35 Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action* (Geneva: International Committee of the Red Cross and Brussels Privacy Hub, 2017), 2nd edition (2020), 3rd edition (2024), https://www.icrc.org/en/document/data-protection-handbook.

It was against this backdrop that the ICRC was framing the update to its Information Environment Strategy for the years 2018–2025 (hereafter, Digital Transformation Strategy). This period also saw the ICRC initiate negotiations with the Swiss Department of Foreign Affairs to amend its 1993 Headquarters Agreement – which governs the ICRC's legal status in Switzerland. The amendments introduced provisions reflecting the digitalisation of the ICRC's activities and the need to better protect its documents, archives, and communications in the digital age, in the interests of victims and their families.[36]

Data Protection as an Enabler for the ICRC's Digital Transformation

The ICRC's analysis of the evolutions and risks in its operating environment informed both the focus of its Institutional Strategy for 2015–2018 and its Digital Transformation Strategy. Several factors were predominant:

- The fast evolution of technology, connectivity and data affecting the way programmes and services could be delivered;
- changing expectations and needs of beneficiaries and other stakeholders;
- requirements in relation to compliance, accountability and personal data protection.[37]

Reinforcing a shift away from data protection as a compliance function, the 48-page Digital Transformation Strategy referenced data protection some 34 times, including as a recently developed "strategic asset", a Guiding Principle,[38] and a core "requirement".[39] The Rules on Personal Data

36 Federal Department of Foreign Affairs, "Switzerland and ICRC Sign Protocol Amending Headquarters Agreement," press release, 27 November 2020, https://www.eda.admin.ch/countries/ireland/en/home/news/news.html/content/eda/en/meta/news/2020/11/27/81392.

37 ICRC, Information Environment Strategy: A Strategy for Information Management, Systems and Technology, IES v.2, (2018–2025) hereafter, Digital Transformation Strategy. Internal document, quoted with permission of the ICRC.

38 The Guiding Principles of the Strategy were designed to "define the way the ICRC information management, systems and technology will evolve. These principles constitute references for decision making" in both annual planning (Planning for Results) and project prioritisation processes. Each principle was weighted to guide prioritisation, with information security and data protection ranked as the second most important. The most important was rationalising and prioritising investments following the ICRC's strategic goals, particularly an assessment in proportion to the value that investments will bring, e.g. to beneficiaries. Internal document, quoted with permission of the ICRC.

39 The Strategy outlines key requirements or undertakings for its implementation to be phased in and to build the necessary foundations for digitalisation. Data protection was specifically

Protection were also referenced in full as an annex. A key rationale for this was the "increasing threats to the rights and freedoms of individuals when it comes from the processing of their personal data through new technologies".

The strong data protection focus was a strategic decision, it was not by chance, and it was thoroughly debated. During the development of the Strategy, its drafts were reviewed by the Directorate, Assembly Council, and the Independent Data Protection Control Commission between July 2016 and August 2018 when it was approved by the ICRC's Assembly.

Data protection was a recurrent theme of discussions within the leadership. A key concern – particularly from the Operations Department – was that data protection requirements posed challenges for the operational response. Discussions often focused on the "overloaded delegate" or the "overcrowded field trip" – raising the question of whether each staff member was expected to fully understand and implement all the data protection rules, or whether specialists were needed on every field trip. The expectation of the Department proposing this was clearly for mainstreaming, as the feasibility – and cost – of hiring specialists for every delegation in the field was never viable. The approach was for a strong core of data protection specialists to support this effort and to foster a broader data protection culture.

Other operational concerns centred on the notion of consent, particularly informed consent in practice, and in relation to the ICRC's Biometric Policy[40] which was being developed. This Policy reflects the evolution of the ICRC's own understanding of the role of data protection, stating:

> *The application of data protection rules to humanitarian action is imperative to safeguard the rights and dignity of individuals, to support the implementation of the "do no harm" principle, and to enhance the accountability and transparency of organizations processing personal data. For the ICRC, the protection of personal data whose disclosure could put its beneficiaries at risk, or otherwise be used for purposes other than those for which it was collected, is*

identified as one of five requirements related to "testing and delivering according to a new methodology". One requirement was dedicated to the respect of the ICRC Rules on Personal Data Protection combined with ICT security assessments when launching new innovation initiatives, projects, or processes to treat and share information, and for mitigation measures to have privacy by design tools and approaches which adequately protect sensitive information and personal data. This requirement also references data minimisation on the basis of a clearly identified and legitimate purpose. Internal document, quoted with permission of the ICRC.

40 ICRC, Policy on the Processing of Biometric Data by the ICRC, adopted 28 August 2019, https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf.

> *an integral means of preserving its neutrality, impartiality, and independence, as well as the exclusively humanitarian nature of its work.*[41]

The Policy aimed to reinforce an informed, researched, and solution-driven data protection approach, responding to operational needs. This was exemplified during the drafting process of the Policy, when concerns about how to manage aid distribution led to the data protection team proposing "a token-based verification credential". This would enable a beneficiary to verify receipt of aid through a token held directly by them without requiring the ICRC to hold their biometric data.[42] This was decisive in creating leadership support for the Policy's adoption.

This period marked an important foundational phase for data protection at the ICRC, positioning it as a key enabler of the organisation's broader ambition for trusted digital transformation. It was still viewed as a complexity, but focus shifted to how to deliver it, and to the associated costs.

Trust, Proximity, Access, and Accessibility Through Digital Transformation

The Value Proposition for Digital Transformation

The Digital Transformation Strategy focused on the ICRC's mandate to protect people, emphasising an approach that recognised the critical importance of data as a risk for individuals in insecure environments. The ICRC aimed to minimise these risks through its own practices whilst also promoting a humanitarian-purpose driven approach to the collection and management of personal data on individuals in such contexts. This commitment was elaborated in a value proposition that served as a central driver of the Strategy and helped determine priority investment areas. It states:

> *The ICRC is recognized as a trusted manager of sensitive information on individuals in insecure environments affected by armed conflict and violence, and on the humanitarian situation. The ICRC endeavours to influence other organizations to follow a humanitarian purpose driven approach to the use of data on vulnerable individuals as the collection and use of data on individuals is a risk factor for their safety ("do no digital harm").*[43]

41 ICRC, Policy on the Processing of Biometric Data, section 1.2.
42 ICRC, Policy on the Processing of Biometric Data, section 5.1.
43 ICRC, Digital Transformation Strategy. Internal document, quoted with permission of the ICRC.

From the ICRC's perspective, the growing ability to collect and analyse large volumes of data in humanitarian crises required a deliberate emphasis on data minimisation – ensuring that only the data strictly necessary was collected – and that it was used solely for the humanitarian purpose for which it was originally gathered. This value proposition aimed to build on the ICRC's traditional working practices regarding protection data and its Rules on Personal Data Protection, enabling greater access to data to strengthen the humanitarian response – while safeguarding sensitive information in accordance with its policies and rules.

In a rare departure for the ICRC, the value proposition also included an ambition to influence other organisations in how data is used to ensure best practices and common standards for the benefit and protection of affected persons. This position evolved from growing external pressure to access granular data not required for reporting and accountability, to share data between humanitarian organisations, and the ability to leverage technology to collect, aggregate, and analyse data on individuals at scale. It also reflected the recognition that humanitarian actors operate within the same ecosystem, and that the policies and practices of one organisation impact the entire sector. The safeguarding crisis had occurred in this period.[44]

The 2019–2024 Institutional Strategy[45] framed the ICRC's level of engagement with digital transformation, dedicating its fifth strategic objective to this goal. This emphasised digital accessibility, meaningful engagement with affected populations and stakeholders, and ensuring that the ICRC remains a trusted manager of personal information. The Strategy further committed to upholding data protection, digital, cyber, and information security standards to safeguard the integrity, confidentiality, and availability of information systems and data.[46]

44 The external environment was a significant influence, particularly following the exposure of a major safeguarding scandal in the humanitarian sector. In February 2018, media reports revealed that Oxfam staff engaged in sexual exploitation while working in Haiti in 2010, with some staff allowed to resign rather than face disciplinary action, leading to intensified scrutiny and a heightened focus by donors on policies to prevent misconduct and ensure compliance.

45 ICRC Institutional Strategy 2019–2022 (Geneva: ICRC, 2019), https://www.icrc.org/sites/default/files/wysiwyg/About/jobs/icrc_institutional_strategy_2019_2022.pdf. The author, serving as an ICRC Director, contributed to the development of the Institutional Strategy, including the choice of key priority areas.

46 ICRC Institutional Strategy. The fifth strategic objective was formulated against the backdrop of the Digital Transformation Strategy, 23.

The Importance of Trust in a Digital Humanitarian Landscape

Trust-building in the digital age was recognised as important to ensure that the ICRC's presence – whether physical or digital – remained credible, accessible, and impactful. During this period, the ICRC commissioned research[47] to explore the drivers of trust as a starting point to assess how the use of technology might affect it. "Trust"[48] – a word used 39 times in the Digital Transformation Strategy – and the responsibility to "do no harm", meaning that its actions do not lead to adverse impacts or create risks for persons and/or communities, were foundational elements of the ICRC's Digital Transformation approach. Proximity to affected populations and other stakeholders was central to the ICRC's protection policy and *modus operandi*, and thus another key driver for the Strategy. Proximity enabled an understanding of local realities and empathy, to shape an appropriate response, and ultimately, to build trust.

Digitalisation challenged the notion of proximity-based protection by introducing proximity through digital tools. The ICRC's Protection Policy stated that "except in special circumstances, the ICRC does not directly carry out protection activities in contexts where it has no access to affected persons and no first-hand knowledge of the situation".[49] The ICRC sought to promote a "more focused people-centric model" that emphasised not only the ability to *access* people but also to be *accessible* to them through its multidisciplinary response. This required that digital tools serve as a complement – not a replacement – for physical proximity, reinforcing rather than diminishing the ICRC's presence and engagement on the ground.[50] This also recognised that there may be access constraints – people not wanting or not being able to access digital responses, and that connectivity may be unavailable, restricted, or manipulated.

47 Commissioned by the author, unpublished. Some elements were brought to a workshop chaired by the author. ICRC and IFRC, Waking the Red Giant: Movement Communications – Alignment and Strategic Importance, report on the workshop at the 2017 Council of Delegates, November 2017, https://rcrcconference.org/app/uploads/2019/06/CoD17-WS5-Communication-report-final-EN.pdf.

48 Trust has traditionally also been reinforced through the ICRC's *modus operandi*, acceptance model, discreet diplomacy and confidentiality, operational impact, transparency and consistency of its action and mandate – alongside its adherence to the Fundamental Principles, particularly humanity, neutrality, independence, and impartiality.

49 ICRC, ICRC protection policy (as published in the International Review of the Red Cross, 2008): 761, https://library.icrc.org/library/search/notice?noticeNr=24634.

50 ICRC, Digital Transformation Strategy. Internal document, quoted with permission of the ICRC.

Trade-offs in the ICRC's Digital Transformation

Digitalisation is transforming the way that the humanitarian sector monitors, engages with, and responds to crises, and this has required an understanding of the trade-offs involved. For the ICRC, financial, legal, and operational trade-offs were outlined in the Digital Transformation Strategy's supporting documents to ensure a shared understanding of the investments and institutional shifts this entailed.

One of the most important trade-offs the ICRC faced was related to technology choices. Risks assessed included the geopolitical perceptions of technology, location of data centres and applicable laws, usability, scalability, encryption, cybersecurity, risk exposure, sovereignty, and the ability to negotiate terms and conditions. In this regard, cloud computing[51] was a key challenge. Although the ICRC was already leveraging a private cloud, scalable digital transformation required a new cloud strategy that addressed the opportunities and risks of private, hybrid, or public[52] cloud options. Trade-offs centred on interoperability, convenience, functionality, and costs versus risks to confidentiality, lack of transparency in processing operations, the potential interception of sensitive information, unauthorised third-party access, limits to control over data, potential implications for the ICRC's privileges and immunities when data processing is outsourced to external cloud service providers, and the risk of vendor lock-in. The Strategy emphasised the need to strengthen and regularly review technology procurement practices "to ensure compliance with internal requirements such as data protection".[53]

Concerns about the associated technological trade-offs led the ICRC to pursue strategic partnerships – such as those established with the Swiss Federal Institutes of Technology in both Lausanne (EPFL)[54] in 2016 and Zurich

51 Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The National Institute of Standards and Technology's Definition of Cloud Computing, September 2011, https://csrc.nist.gov/pubs/sp/800/145/final.

52 A private cloud is operated solely for a single organisation, whether managed internally or by a third party, and hosted either internally or externally. Public cloud services are rendered over a network that is open for public use. A community cloud is jointly available to a number of organisations that share common interests, concerns and/or requirements. A hybrid cloud is a composition of two or more clouds that remain distinct entities but are bound together, offering the benefits of multiple deployment methods. ICRC, *Handbook on Data Protection*, 149–150.

53 ICRC, Digital Transformation Strategy. Internal document, quoted with permission of the ICRC.

54 On 8 March 2016, the ICRC and EPFL launched the Humanitarian Tech Hub with one of its stated aims "to develop technologies to tackle the humanitarian challenges facing

(ETH) in 2020[55] – to "bridge the gap between emerging technologies and the pressing needs of vulnerable populations affected by conflicts".[56] Whilst it was recognised that this would not provide short-term solutions, it allowed the ICRC to deepen its understanding of emerging technologies and research solutions. Exemplifying this, EPFL's research to assess the ICRC's computer security needs from operational, technical, legal, and managerial perspectives confirmed challenges related to data security and privacy throughout the data lifecycle, and trade-offs between "operational security and requirements …".[57]

Other trade-offs identified were related to resourcing and prioritisation; control versus collaboration, distinguishing what the ICRC was – and was not – comfortable carrying out with others; and balancing the focus on digitalisation with the stability of existing systems.

A strong focus on data protection also came with trade-offs. Robust risk assessments, privacy by design, and informed consent resulted in a slower rollout of services and increased costs. The ICRC made a trade-off between the pace of innovation and risk minimisation. This is evident in its incremental approach to the development and rollout of RedSafe,[58] originally validated in the 2018 Digital Transformation Strategy and initially deployed in one country in 2021 following three years of development, testing, and adherence to data protection requirements. Similarly, its policy-led stance on biometrics favoured tokenisation over widespread collection of biometric data.

The RedSafe platform and the Biometrics Policy offer strong illustrations of how the ICRC has actively navigated and addressed some of the complex trade-offs inherent in the use of digital technologies in humanitarian action. Through the identification of potential risks and benefits, the ICRC has demonstrated deliberate and principled decision-making processes – balancing operational needs with the imperative to protect individuals' rights and dignity. RedSafe integrates strong data protection measures, reflecting a cautious approach to digital service delivery. The Biometrics Policy articulates clear boundaries and conditions under which biometric data may be collected and used, emphasising necessity, proportionality, and respect for individual agency.

---

the world today", https://www.icrc.org/en/document/icrc-and-epfl-launch-humanitarian-tech-hub.

55 Engineering for Humanitarian Action, "Home," accessed 25 April 2025, https://eha.swiss/.

56 Bridging the Gap between Humanitarian Needs and Technological Innovation, https://eha.swiss/about/.

57 Stevens Le Blond et al., "On Enforcing the Digital Immunity of a Large Humanitarian Organization," *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, 424–440. https://ieeexplore.ieee.org/document/8418617.

58 ICRC, RedSafe, a Digital Humanitarian Platform, https://www.icrc.org/en/redsafe.

Conclusion: People Before Technology

The ICRC's digital transformation marked a fundamental shift from viewing ICT as a back-office function to recognising its role in the delivery of humanitarian action. At the heart of this transformation was data protection, framed as both a compliance necessity and an enabler of the protection of individuals. Shaped by the urgency of establishing a data protection framework during a time of rapid regulatory evolution, the ICRC's core programmes – such as Restoring Family Links – would have faced significant constraints without its introduction, including limitations on data sharing with the ICRC. The early decision to align with international standards, including the GDPR, strengthened the ICRC's ability to operate across jurisdictions and interface effectively with external stakeholders.

Over time, data protection demonstrated its value beyond compliance, serving as an enabler to understand the risks during a period when the hype and opportunity of technology were overwhelming. It became a foundation for how data should be collected, used, shared, stored, and deleted – in a way that aims to uphold individuals' rights, integrity, dignity, and safety – reinforcing the ICRC's Protection Policy. The ICRC's Handbook on Data Protection in Humanitarian Action has set a sector-wide benchmark for practical, people-centric, rights-based guidance on the responsible use of technology, much as its Protection Standards, including for missing persons, did in previous decades.

Its practical value became clear in the field, where teams were the first to face questions from National Societies and authorities that the data protection team supported them in addressing. With hindsight, this could have been facilitated by a stronger framing of existing Protection and Health Standards to underscore its importance for the ICRC's action.

Implementing the ICRC's Rules on Personal Data Protection required not only a review of the implications of technology use, but also the development of new policies on biometric data, cloud services, and third-party partnerships. The strategy remained technology-agnostic – deliberately distanced from digital hype – and focused instead on the people behind the data. This helped balance speed with safety, innovation with responsibility, and impact with privacy at a time when "privacy is dead"[59] was a popular refrain.

Digital transformation has significantly increased the volume of personal data handled by humanitarian organisations. This shift has created ethical, legal, and operational challenges, requiring investment in cyber resilience and informed responses to emerging threats. The complexity of sound technology

59 See for example, Jean-Pierre Hubaux, and Ari Juels, "Privacy is Dead. Long Live Privacy!" *Computer Science at Furman University*, 2015, https://cs.furman.edu/~tallen/csc271/source/privacyDead.pdf.

decisions – especially where no ideal solutions exist – reinforces the need for robust governance and internal capacity.

Importantly, data protection has reinforced the need to understand the humanitarian principle of "do no harm" in the digital sphere. Humanitarian organisations must exercise due diligence in safeguarding data and information systems – not merely as a compliance requirement, but as a fundamental obligation to uphold the principle of "do no harm" to the populations they serve.

The ICRC's commitment to proximity, access, and accessibility in a digital age aimed to reinforce trust-building. Whether it succeeded in doing so remains to be assessed. The reality is: digital transformation is not about technology – it is about data, people, and the systems that connect them. It changes how aid is delivered, how communities are engaged, and how humanitarian principles are upheld in an increasingly connected world. As the means to collect, aggregate, and analyse data continue to evolve at speed, risks and ethical dilemmas persist, and humanitarian actors must continue investing in data protection, cybersecurity, and privacy-preserving innovations. There are no shortcuts. Digitalisation, ultimately, must serve people – not systems.

PART 3

Data Protection at the Crossroads

PART 3.1

Evolution of Data Protection and Humanitarian Action in International Law and Diplomacy

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

8

DATA PROTECTION REGULATION AND INTERNATIONAL HUMANITARIAN ORGANISATIONS

Revisiting the Origins, Nature and Significance of the UN Guidelines on Personal Data Regulation (1990)

David Erdos

Introduction[1]

This publication is timed to mark a decade since the adoption by both the International Committee of the Red Cross (ICRC) and the United Nations (UN) High Commissioner for Refugees (UNHCR) of rules/policies on personal data protection,[2] as well as the Resolution on Privacy and International Humanitarian Action by the International Conference of Data Protection and Privacy Commissioners that same year.[3] That these initiatives took place just as the European Union (EU) was negotiating its General Data Protection Regulation (GDPR) can be taken to indicate that it is potential or actual 'bilateral' pressure (whether from a State or a supranational organisation such as the EU) which has proved most crucial to the establishment of data

1 I would particularly like to thank Alex Novikau for his help in locating UNHCR documents from the 1990s and 2000s as cited in footnotes 40 and 53 below.

2 ICRC, "ICRC Rules on Personal Data Protection," (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html; and UNHCR, "Policy on the Protection of Personal Data of Persons of Concern to UNHCR," (2015), https://www.refworld.org/policy/strategy/unhcr/2015/en/120873. Although the ICRC rules were truly comprehensive, the UNHCR Policy had a narrower scope and it was not until December 2022 that a general policy was introduced, with full implementation delayed until December 2025. See UNHCR, "General Policy on Personal Data Protection and Privacy," (2022), s. 77, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207.

3 International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy and International Humanitarian Action," (2015), https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

DOI: 10.4324/9781003650164-13

protection within this area[4] and, furthermore, that this only has a recent history. Nevertheless, as the 2015 Commissioners' Conference Resolution itself indicates, bilateral action has taken place against the background of much wider multilateral debate and initiative. Moreover, as this paper will elucidate, this kind of debate and initiative has a much longer history stretching back to the decade-long development of the UN General Assembly's Guidelines for the Regulation of Computerized Personal Data Files (UN Guidelines)[5] which were adopted by the UN General Assembly through Resolution 45/95 on 14 December 1990.

The UN Guidelines clearly seek to establish a universally applicable scheme to govern the computerised handling of personal data. Nevertheless, they particularly focus on international organisations (IOs) and, most especially, those pursuing a humanitarian task. At the same time, even within the UN system itself, the commanding force of the UN Guidelines in and of themselves has been (and remains) rather limited. Thus, as this chapter will show, no example can be found of an IO generally adopting the Guidelines either during the 1980s when they were in draft form or in the 1990s when the UN Commission on Human Rights engaged in a years-long follow-up exercise on the implementation of the final version. Indeed, Interpol remains the only example of a truly international governmental organisation which enacted comprehensive data protection during this entire period. This was finalised in 1985 and was clearly catalysed not by initiatives at the UN but rather by 'bilateral' pressure from their headquarters country (namely, France).[6] Nevertheless, at least as regards governmental IOs and especially those with a 'humanitarian' task, the drafting and reality of the UN Guidelines have been far from irrelevant. To the contrary, they have provided a broadly phrased, principles-based normative framework for governmental IOs to apply in their personal data governance and, as regards humanitarian IOs, have established the normative expectation of a "humanitarian clause" enabling derogations

4 It is clear that at least the ICRC saw the adoption of the GDPR as risking much more external pressure on its approach to data protection. See Council of the EU. Document 7355/15 (25 March 2015), https://data.consilium.europa.eu/doc/document/ST-7355-2015-INIT/en/pdf and Council of EU, *Document 8837/15* (12 May 2015), https://data.consilium.europa.eu/doc/document/ST-8837-2015-INIT/en/pdf. It therefore appears likely that such pressure also galvanised the internal development of data protection protocols and supervision.

5 "Guidelines for the Regulation of Computerized Personal Data Files: Adopted by General Assembly resolution 45/95 of 14 December 1990," https://www.refworld.org/policy/legalguidance/unga/1990/en/13761.

6 See G Russell, "Interpol-France Accord Signals Records Supervision Action," *Transnational Data Report* 7, no. 2 (1985): 62 (noting that a new Headquarters Agreement, including binding data protection provisions, had been negotiated at the urging of the French Data Protection Authority). This case is discussed further in the subsequent section on Drafting the UN Guidelines: International Organisations and the 'Humanitarian Clause'.

when the purpose of the file (or, in more modern parlance, processing) "is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance". Such influence remains clear to this day. In particular, both the ICRC and UNHCR rules/policy remain broadly phrased, their restrictions/derogations provisions have clearly been influenced by the Guidelines' "humanitarian clause",[7] and UNHCR policy as applied to refugees and other persons of concern to it explicitly references ensuring conformity with the UN Guidelines as a core purpose.[8] Meanwhile, local instruments such as the EU GDPR now recognise the special position of "humanitarian purposes" or "international humanitarian organisation[s]" as regards lawfulness, derogations, or restrictions from general provisions and transborder data transfers.[9]

This chapter explores the nature and significance of the adoption of the UN Guidelines by humanitarian IOs, as well as the limitations present here. It particularly seeks to uncover the origins of the key norms authoritatively promulgated, highlighting the strategic position and entrepreneurship of Louis Joinet and the advocacy of groups such as UNHCR and, most especially, Amnesty International. The chapter is structured into four further sections. The following two examine the drafting of the UN Guidelines both in general and, more especially, as regards IOs and especially those IOs with 'humanitarian' purposes. Focusing especially on the position of humanitarian IOs, the chapter then explores the formal follow-up on the implementation of the UN Guidelines during the 1990s. Finally, the last section analyses these findings and sets out some broader conclusions.

Drafting the UN Guidelines: An Overview

UN involvement in data protection traces back to the very earliest development of this legal and policy framework. Following the Tehran International Conference on Human Rights, in 1968 the UN General Assembly adopted Resolution 2450 (XXIII), which called on the UN Secretary-General to study "the problems in connexion with human rights arising from developments in science and technology", in particular as regards "[r]espect for the privacy of individuals" and the "[u]ses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society". However, although several interesting reports were forthcoming, the "ideological divisions" of the Cold War and the dominance

7 UNHCR, "General Policy," s. 64; ICRC, "Rules," art. 14 (which explicitly references "ICRC's humanitarian mandate").

8 UNHCR, "Policy on the Protection of Personal Data of Persons of Concern to UNHCR," s. 1.1.

9 EU General Data Protection Regulation 2016/679, Recitals 46, 73, and 112.

of a "South/East camp" at the UN "pushed the matter to the edges".[10] Notwithstanding a Western boycott (and eventual abstention), in 1975 the General Assembly adopted a rather different and substantive "Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind" (Declaration 3384 (XXX)). This Declaration predominantly focused on other concerns, including prohibiting the use of science and technology "for the purposes of violating the sovereignty and territorial integrity of other states, interfering with their internal affairs, waging aggressive wars [or] suppressing national liberation movements" as well as ensuring the "strengthening and development of scientific and technological capacity of developing countries". These sorts of issues continued to dominate formal UN discussions in this area right up until the enactment of the UN Guidelines in 1990. However, although the 1975 Declaration's "reference to human rights and privacy, in particular, [was] largely remote",[11] it nevertheless did remain a part of the UN's agenda as regards scientific and technological developments, including computerisation.

In 1980 the UN Commission on Human Rights' Sub-Commission on Prevention of Discrimination and Protection of Minorities finally commissioned a study on relevant guidelines related to "grave risks of interference with the privacy of individuals and the exercise of their freedoms" posed by the "concentration of personal particulars" into "computerized personal files". The study was to produce guidelines and "state members of the UN and international, intergovernmental or regional agencies using data processing" were to be invited to adopt "rules of protection" based on these.[12] Louis Joinet had prepared this resolution[13] and the Chairman of this Sub-Commission assigned the task of completing the study to the French delegate on the understanding that her alternate, who was Louis Joinet, would undertake it. Joinet himself became the French delegate on this body shortly thereafter[14] and remained the Sub-Commission's Special Rapporteur on this topic throughout the period leading up to the UN Guidelines being finalised. Joinet was an inaugural Director of the French Data Protection Authority – the *Commission Nationale de l'Informatique et des Libertés* (CNIL), between

10 Micheal Kinfe, "The United Nations data privacy system and its limits," *International Review of Law, Computers and Technology*, 33, no. 2 (2019): 226, http://dx.doi.org/10.1080/13600869.2018.1426305.

11 Micheal Kinfe, "The United Nations data privacy system and its limits," 227.

12 See Resolution 12 (XXXIII) as reprinted below Andrew Lloyd, "UN Takes Up Data Protection," *Transnational Data Report* 4, no. 1 (1981): 11.

13 Andrew Lloyd, "UN Takes Up Data Protection".

14 "Study of relevant guidelines in the field of computerized personnel [*sic*] files: Final report prepared by Mr. Louis Joinet," (E/CN.4/Sub.2/1983/18), 2, https://digitallibrary.un.org/record/54917?ln=en&v=pdf.

1978 and 1980[15] (and had also been one of the authors of the official report which led to France's first data protection legislation).[16] He, therefore, brought to this task a wide knowledge of data protection developments internationally and, in particular, within his home country.

Following the presentation of an interim draft in 1981, Joinet's initial study of guidelines in this area was completed in June 1983.[17] Although predominantly descriptive, the broad outlines of what would become the UN Guidelines were clear even at this point. Subject to certain exceptions,[18] Joinet proposed that States should "take steps to give effect to" a set of "basic [data protection] principles"[19] applying at least to computerised files containing personal data within both the public and private sectors. Those IOs which did not accept local jurisdiction were to adopt their own protective measures based on the same principles. The principles related to "fairness, accuracy, purpose specification, openness, individual access and security"[20] and closely mirrored the Council of Europe's Data Protection Convention[21] which was finalised in 1981 and which Joinet had direct experience of helping draft. Both the Sub-Commission and the Commission on Human Rights welcomed Joinet's study, and in August 1984 the Sub-Commission asked the UN Secretary-General to forward the provisional draft guidelines to States and also to all relevant IOs and request their views. Although this was carried out by November 1984, few replies were forthcoming and so, following further requests, follow-ups were sent by the Secretary-General in November 1985 and April 1987.[22] Joinet presented the Sub-Commission with a final Report and a finalised set of Guidelines in July 1988.[23] These draft Guidelines were forwarded on 1 September 1988 by the Sub-Commission to the Commission on Human Rights, by the Commission to the UN Economic and Social Council on 6 March 1989, and finally by the Council to the UN General Assembly on 24 May 1989 with a new request to States to submit comments by 1 September 1989. The response of States continued

15 Emmanuel Decaux, "In memoriam Louis Joinet (1934–2019)" (2020), https://www.crdh.fr/revue/n-18-2020/in-memoriam-louis-joinet-1934-2019/.

16 "*Rapport de la Commission Informatique et Libertés*" (1975), 100, https://www.cnil.fr/sites/cnil/files/atoms/files/rapport_tricot_1975_vd.pdf.

17 "Study of relevant guidelines," 2.

18 "Study of relevant guidelines," 19–20.

19 "Study of relevant guidelines," 23.

20 "Study of relevant guidelines," 24.

21 Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

22 "Guidelines for the regulation of computerized personal data files: Final report submitted by Mr. Louis Joinet, Special Rapporteur," (E/CN.4/Sub.2/1988/22), 2, https://digitallibrary.un.org/record/43365?ln=en.

23 "Guidelines for the regulation of computerized personal data files".

to be disappointing. Indeed, by the end of September, replies to the latest request had only been forthcoming from seven States (all Western European other than Burundi and Japan),[24] although two further replies (from Austria and Canada) were sent in by the end of the year.[25] On 5 December 1989, the General Assembly through Resolution 44/132 invited Joinet to take into account these comments and to submit a revised version of the Guidelines. Finally, on 14 December 1990, the UN General Assembly passed, without a vote, Resolution 45/95 which, *inter alia*, adopted this revised version of the Guidelines, requested that Governments take them into account "in their legislation and administrative regulations" and also requested "governmental, intergovernmental and non-governmental organizations to respect those guidelines in carrying out the activities within their field of competence".[26]

Drafting the UN Guidelines: International Organisations and the 'Humanitarian Clause'

It does not appear that the main UN debates and reports of the late 1960s and 1970s gave any significant consideration to the particular position of IOs. In contrast, despite the manifestly wider (and indeed comprehensive) ambitions of the Sub-Commission on Prevention of Discrimination and Protection of Minorities, this did become a special focus right from the moment this Sub-Commission took up the question of data protection in 1980. In sum, not only were IOs directly mentioned in the Sub-Commission's resolution[27] but Joinet explicitly flagged the personal data activities of Interpol, the ICRC, UNHCR, and the World Health Organization and "concern" was reported from Sub-Commission members at "the fact that a growing number of personal data files were being compiled by international agencies". It seems likely that part of the reason for this refocusing was to deflect attention from the much more divisive issues concerning the regulation (or lack thereof) of personal data by States themselves and, in particular, whether laws restricting the transfer of personal data between them were or were not justified. Indeed, the Resolution passed by the Sub-Commission at this point avoided all mention

24 "Guidelines for the regulation of computerized personal data files: Report of the Secretary-General," (A/44/606) (24 October 1989), 2, https://digitallibrary.un.org/record/79050?ln=en&v=pdf.

25 "Guidelines for the regulation of computerized personal data files: Report of the Secretary-General," (A/44/606/Add.1) (15 December 1989), https://digitallibrary.un.org/record/83364?ln=en&v=pdf.

26 General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files: Resolution," (14 December 1990), https://digitallibrary.un.org/record/105299?v=pdf.

27 Resolution 12 (XXXIII) as reprinted below Lloyd, "UN Takes Up Data Protection".

of transborder data flows, with Joinet explicitly stating that this was "to avoid the immediate re-emergence of old disagreements".[28]

In one of the three main parts of his 1983 study, Joinet provided an analytical description of the state-of-play regarding IOs. The "files" at issue were divided into "those relating to the organization's internal procedures" (labelled "internal") and those "intended to enable the organisation to achieve greater efficiency in carrying out its statutory tasks" (labelled "external"). Save for one exceptional IO, Joinet found that "external" files had not been the subject of any "protective measures" and that, even as regards "internal" files, only four organisations had intervened by making "certain files" subject to "an individual right of access by the organization's staff members".[29]

The exceptional case noted was Interpol which, through an exchange of letters with the host of its headquarters (namely, France), was establishing a general system of oversight through a multinational supervisory commission charged with ensuring that specified "[r]ules" regarding personal data were adhered to and enabling an "indirect right of access" for those who were citizens or residents of Interpol Member States.[30] The background to this agreement lay in an understanding that even a governmental IO was "in principle subject to the territorial jurisdiction of the country of its headquarters" save for any "headquarters agreement granting privileges and immunities". Interpol's agreement with France which dated from 1972 had made "no provision" on "the supervision of files" and, with the advent of data protection legislation in France from 1978, the CNIL had taken the view that unless this agreement was renegotiated "French law applied".[31] It was this renegotiation which led to a new agreement to establish new rules and supervisory machinery.[32] Joinet stressed that Interpol's problems were in fact general ones since "[t]he existing headquarters agreements [for IOs] did not … foresee the emergence of these new legislative provisions relating to data processing and freedoms". He also suggested that "subject to some adaptations or improvements" Interpol's new arrangements "constitute[d] a valuable precedent and may serve as a framework of reference" for other IOs.[33] This finding undergirded Joinet's ultimate recommendation that, save where they "accept[ed] local jurisdiction where such exists", IOs using "computerized personnel files" should adopt "internal

28 Lloyd, "United Nations Takes Up Data Protection".

29 "Study of relevant guidelines," 21–22.

30 "Study of relevant guidelines," 22–23.

31 "Study of relevant guidelines," 22. During 1981, Interpol had accepted such direct jurisdiction by the French data protection authority as regards the files it maintained on French citizens. See "Interpol Accepts Data Protection Access," *Transnational Data Report* 3, no. 8 (1981): 1. However, discussions clearly continued as regards a more comprehensive, long-term solution.

32 This agreement was finalised and entered into force in 1985 (see *supra* note 6).

33 "Study of relevant guidelines," 22–23.

statutes and rules" including the set of protective "principles" and set out a "supervisory authority" with advisory and enforcement tasks which offered "adequate guarantees of impartiality".[34]

Despite the strong focus on IOs and similar organisations, the 1983 Report included no mention of the special problems faced by those IOs with specifically 'humanitarian' tasks. This is somewhat surprising since Joinet *was* clearly particularly concerned about the regulation of files for "external use" and all the particular examples he cited in this context related back to 'humanitarian' tasks broadly conceived, namely, "files on refugees" of UNHCR, a file in the UN Centre for Human Rights "on victims of enforced or involuntary disappearances", and "[c]ertain applications" by the ICRC and also "the non-governmental organization Amnesty International".[35] Nevertheless, a different section of the Report did examine the positive "use" made of "[c]omputerized data files" by "organizations specializing in the protection of human rights" where it was acknowledged that "[p]rovided specific protective measures are taken" such developments were of "great interest", including in "resolving more efficiently certain administrative problems during the introduction and implementation of action programmes in support of refugees or displaced persons".[36] As the reference to Amnesty International in the IO section reveals, Joinet was aware of both the overlaps and problems here. It also appears that both Amnesty International and the ICRC later brought these issues to the 1983 International Data Protection Commissioners' Conference which, responding sympathetically, had decided to establish a sub-committee on various substantive and jurisdictional issues arising. The 1983 Conference made this sub-committee "a continuing body of the conference" with a remit "to deal with *bona fide* international organizations pursuing humanitarian goals or defending human rights on an international basis, such as Amnesty International or the International Red Cross" and with an objective "to attempt to find a solution within international public law corresponding to the activities of those organizations and their need for security and confidentiality".[37] However, although this sub-committee continued its work until 1988, the Commissioners' Conference of that year revealed that it ultimately achieved little decisive.[38]

34 "Study of relevant guidelines," 24–25.

35 "Study of relevant guidelines," 21.

36 "Study of relevant guidelines," 9.

37 Tom Riley, "Data Commissioners Review International Problems," *Transnational Data Report* 6, no. 8 (1983): 414.

38 Noting that it had adopted an internal code of privacy principles in 1985, a representative of Amnesty International at this Conference stated that it required exemption from domestic data protection laws as it needed "the right to be allowed to exchange information through computers, internationally and with no barriers imposed by existing legislation". However, although sympathetic, the Conference did not support this but merely

Largely mirroring the 1983 Report, Joinet's final Report to the Sub-Commission in June 1988 proposed that governmental IOs should apply the revised set of guidelines to their own personal data files (albeit subject to possible adjustment to take account of potential differences between "internal" and "external" files) and should also designate a "statutorily competent" supervisory authority[39] (although, in light of the diversity of opinion on this point, the nature of such an authority was not specified).[40] The Report also provided an updated description of IOs' approach to files containing personal data which, given that Interpol clearly remained the only governmental IO which had adopted a comprehensive approach here,[41] rather charitably stated that "many international organizations, in conformity with the proposals of the Special Rapporteur, have taken initiatives at the internal level".[42] UNHCR was even stated to be "engaged in setting up internal protective machinery" "in co-operation with the Special Rapporteur".[43]

In contrast to the 1983 Report, Joinet's final Report of June 1988 also included specific discussion of the particular issues arising for humanitarian IOs. This discussion arose specifically from concerns voiced both by Amnesty International and UNHCR[44] on the proposed "general rule" (ultimately reflected in the final Guidelines as the "Principle of non-discrimination"[45]) prohibiting the compilation of information raising the risk of "unlawful or arbitrary discrimination", including such sensitive data categories as "racial or ethnic origin", "political opinions, religious, philosophical or other beliefs", and "membership of associations or trade unions". Joinet agreed that a "total ban" on the collection of such information "might frustrate the goal sought when the purpose of the compilation is to end a violation of the rights of

---

held that "if problems arose they would be dealt with on a case-by-case basis". See "Data Commissions Consider Wider Horizon," Transnational Data and Communications Report, 11 (December 1988): 11.

39 "Guidelines for the regulation," (E/CN.4/Sub.2/1988/22), 11–12.

40 "Guidelines for the regulation," 9.

41 Amnesty International, as a non-governmental IO, had apparently adopted a relatively comprehensive approach in 1985 (see *supra* note 38). However, this appeared to be unknown to Joinet, who merely acknowledged its international efforts over four years to promote "the adoption of standards for the files of organizations at work in the field of human rights and humanitarian activities, especially the adoption of a 'humanitarian clause'".

42 "Guidelines for the regulation," 7–9.

43 "Guidelines for the regulation," 8. Although such machinery apparently did not come to fruition, on 12 February 1990, UNHCR did adopt a two-page policy on the "Confidentiality of information concerning individual refugees or asylum-seekers in discussions with countries of origin" (UNHCR/IOM/12/90).

44 The only other obviously humanitarian organisation which responded to Joinet's consultation was the UN Centre for Social Development and Humanitarian Affairs ("Guidelines for the regulation," 13).

45 UN Guidelines, Principle 5.

an individual". Recognising that these cases would anyway fall within the envisaged right to make "necessary" exceptions for protecting "rights and freedoms",[46] he proposed that this issue be dealt with explicitly through a "humanitarian clause". Although the proposal as discussed appeared to be confined to the non-discrimination principle and was described as merely "allowing the power to make exceptions",[47] the actual text went much further by extending the derogation to the principles as a whole and by placing States under a positive obligation to make such exemptions available for all governmental and even non-governmental 'humanitarian' IOs. In sum, those IOs with self-jurisdiction could, through a "humanitarian clause", establish derogations "when the purpose of the right is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance". In contrast, it was positively stated that "similar provision *should* be provided in national legislation" (emphasis added) which would cover "governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation"[48] and even "non-governmental international organizations" such as Amnesty International.

Subsequent intergovernmental consultations included little of direct relevance to IOs or humanitarian issues. The "humanitarian clause" was noted by Austria "with particular interest and satisfaction" (and was, perhaps optimistically, held to be "fully compatible" with its legislation).[49] Meanwhile, although Norway proposed that IOs "filing sensitive data" should register their adherence to the guidelines at the UN and "an authority to supervise" observance should be created within the UN,[50] this was not adopted. Therefore, as regards IOs and humanitarian IOs specifically, the Guidelines as adopted by the UN in December 1990 were (with minor rewordings) the same as those proposed in the 1988 Report and as elucidated above.

Formal Follow-up on UN Guidelines during 1990s

On 10 March 1993, the UN Commission on Human Rights requested that the UN Secretary-General report to the Commission at its 51st Session in early 1995 on the application of the Guidelines within the UN system and, through the collection of information from intergovernmental, regional and non-governmental organisations, on their follow-up at the regional and national levels. Although in May 1994 such information was requested from within the

46 UN Guidelines, Principle 6.
47 "Guidelines for the regulation," 5–6.
48 "Guidelines for the regulation," 12.
49 "Guidelines for the regulation," (A/44/606/Add.1), 1.
50 "Guidelines for the regulation," (A/44/606), 8.

UN system and beyond, replies were disappointing. In total, alongside only 13 Governments, responses were received from just ten out of the 62 UN organisations addressed as well as three other intergovernmental organisations.[51] None of these had a specifically humanitarian mandate. There were no replies at all from non-governmental organisations.[52] At its 1995 session, the Commission therefore requested both that the Secretary-General "continue to ensure the implementation of the guidelines in the United Nations system" and that he carry out the information-gathering exercise again and report to the Commission's 53rd session in early 1997. An information request was duly issued in July 1996, but responses were again underwhelming. In total, just 14 Governments responded[53] as well as 12 of the 33 UN organisations the Secretary-General had addressed. Although one of these, namely the UN Department of Humanitarian Affairs, did have a humanitarian mandate, it merely "stated that they had no relevant information to submit or comments to offer with regard to the issue in question". The only reply received from a non-UN intergovernmental organisation (the Organization of American States) similarly stated that it was unable to provide the requested information. There were again no replies at all from non-governmental organisations.[54] In 1997 the Commission re-tasked the Secretary-General not only with ensuring implementation of the guidelines within the UN system but also with carrying out a repeated information-gathering exercise. The Secretary-General issued a new information request in August 1997, but the response was even more disappointing than previously. No Government or (it would appear) non-UN intergovernmental organisation replied, just one non-governmental organisation (namely, the International Federation of Human Rights) did so,

51 Namely, the African Commission on Human and Peoples' Rights, the Council of Europe and Interpol. The Council of Europe's response was from the European Commission on Human Rights (a body with responsibilities under the European Convention on Human Rights), which may help explain why it made no mention either of the Council of Europe's Data Protection Convention (*supra* note 21) or the fact that the Council of Europe (outside of data used in the framework of the European Convention on Human Rights) had established a comprehensive system of personal data protection as regards its own personal data files in 1989. See Council of Europe. "Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe," https://web.archive.org/web/20201015100313/https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680684608.

52 "Question of the follow-up to the guidelines for the regulation of computerized personal data files: Report of the Secretary-General prepared pursuant to Commission decision 1993/113," (E/CN.4/1995/75) (23 December 1994): 3, https://digitallibrary.un.org/record/168863?ln=en.

53 Almost half of these had been respondents to the previous exercise.

54 "Question of the follow-up to the guidelines for the regulation of computerized personal data files: report of the Secretary-General prepared pursuant to Commission decision 1995/114," (E/CN.4/1997/67) (23 January 1997): 2–3, https://digitallibrary.un.org/record/238368?ln=en&v=pdf.

and there were responses from only six UN organisations (only four of which were in any sense substantive). The response of the International Federation of Human Rights did not address its own data processing or otherwise address humanitarian issues, but one UN humanitarian agency, namely UNHCR, did provide a substantive response which, although still rather basic, was still one of the most comprehensive received from a UN agency throughout the entire follow-up exercise. It is elucidated further below. The Commission at its session in 1999 removed the question of follow-up from its agenda (purportedly on the grounds that the guidelines were "progressively being taken into consideration by States") and, without even addressing the position of non-UN IOs, requested the UN Secretary-General "to entrust the competent inspection bodies the task of ensuring the implementation of the guidelines … within the United Nations system".[55]

Turning to the detail of the information provided by UNHCR in 1998, this agency (somewhat implausibly) asserted that its collection of personal data was confined to just three categories of person, namely, (i) personnel (which it classed as "internal" in nature), and (ii) asylum seekers and (iii) refugees and internally displaced persons (both of which it classed as "external"). It acknowledged that it did *not* have specific directives covering all aspects of the Guidelines, citing in particular the lack of directives either on the exactness (i.e. accuracy) of data or the right of file access for individuals. It additionally stressed that it could not comply with what it saw as Joinet's recommendation not to collect information on political persuasions or beliefs, given that "information regarding political affiliation or religious conviction may be pertinent to refugee status determination". Despite clearly lacking a comprehensive approach, UNHCR did flag the presence of a range of relevant specific directives including those on archives and records management, providing for the confidentiality and restriction of access to personnel files and establishing the right of staff members to examine their official status file once a year. As regards files on refugees, asylum seekers, and internally displaced persons, the submission similarly stated that UNHCR directives specified and limited those personnel who could have access to computerised data on refugees, that a wide range of information concerning refugees, internally displaced persons, and asylum seekers was protected by confidentiality and/or a prohibition on disclosure (including an individual's identity, political involvement, and their family, colleagues, and friends), and that publication

55 Commission on Human Rights Report on the Fifty-Fifth Session (E/CN.4/1999/167) (22 March–30 April 1999): 288, https://digitallibrary.un.org/record/287570?ln=en&v=pdf.

of the photographs of such persons was prohibited without explicit consent obtained after due counselling.[56]

Conclusions and Significance

As revealed in the previous sections, the UN Guidelines did not have a direct commanding force either during the period of their gestation in the 1980s or during their formal follow-up in the 1990s. This is clearly apparent in relation to UN Member States, who overwhelmingly remained disengaged throughout both the drafting and the follow-up period. Although a significant number of these States were adopting comprehensive data protection laws by the end of this period, this was clearly catalysed by factors other than the UN Guidelines, including, most notably, the agreement on and subsequent coming into force of the EU's Data Protection Directive 95/46. Notwithstanding that the UN Guidelines and their follow-up particularly focused on IOs within the UN system and, most especially, those with humanitarian purposes, disengagement is apparent in these areas too. Thus, not only did the great majority of IOs, even within the UN system, not respond to the follow-up, but an analysis of those which did shows that *none* had adopted a genuinely comprehensive approach to data protection by the end of the 1990s. Moreover, the only truly international governmental organisation which *had* adopted such comprehensive data protection,[57] namely Interpol as early as 1982, had not acted as a result of UN influence but rather from 'bilateral' pressure exerted by its host country (namely, France through the CNIL, its data protection authority).

Nevertheless, at least as regards IOs and especially humanitarian IOs, the norms instanced within the UN Guidelines remain significant and an understanding of the process of individual and group action which led to this outcome also remains of contemporary relevance. Firstly, the Guidelines were the first instrument to authoritatively set out a structure for data protection

56 As stated at *supra* note 43, in February 1990 UNHCR had adopted a specific policy on refugees and asylum-seekers which concerned confidentiality but only as regards discussions with their countries of origin. On 24 August 2001, broader "UNHCR Guidelines on the Sharing of Information on Individuals Cases ("Confidentiality Guidelines")" (UNHCR Inter-Office Memorandum No. 71/2001) were adopted. This was the precursor to the "Policy on the Protection of Personal Data of Persons of Concern to UNHCR" adopted in 2015. It was not until late 2022 that a truly comprehensive policy was finalised, with full implementation delayed until the end of 2025 (see *supra* note 2).

57 Note that (with the exception of data used within the framework of the European Convention on Human Rights) the Council of Europe had also adopted a comprehensive approach by 1989 (see *supra* note 51). However, this was clearly the result of internal Council of Europe developments (notably, its Data Protection Convention had come into force in 1985) and therefore was also not a result of the UN initiative.

under which governmental IOs might retain substantial autonomy in data protection whilst adhering to a common set of broadly framed principles.[58] Secondly, when such IOs were pursuing 'humanitarian' purposes, it explicitly recognised the need for wide derogations (especially as regards the rules of sensitive/special category data) in order to ensure that such purposes were not unduly hindered. Notably, the expectation set down within this 'humanitarian clause' was explicitly extended to non-governmental as well as governmental IOs. The special focus of the Guidelines on humanitarian IOs was reflective of a range of factors which paradoxically may have indicated a desire to shift the gaze away from yet more controversial intra-state transborder data flows. Nevertheless, it was principally the result of the strategic position and individual entrepreneurship of Louis Joinet as Special Rapporteur operating alongside the advocacy of bodies such as UNHCR and Amnesty International. Thus, not only did both of these bodies raise serious substantive concerns, but the repeated intervention of Amnesty International was almost certainly decisive in ensuring that non-governmental as well as governmental IOs were included within the scope of the 'humanitarian clause' set out in the UN Guidelines. Meanwhile, not least as a result of his connection to the CNIL and its engagement with Interpol, Joinet was strongly committed to including IOs within the emerging system of data protection. At the same time, he displayed a keen appreciation of the importance of humanitarian action (broadly conceived) and the very real danger of inappropriate data protection restrictions unduly impeding (or even preventing) such action.

Although a detailed study of this goes beyond the scope of this chapter, it is also clear that the UN Guidelines did come to exert a significant influence when (often much later) governmental IOs pursuing humanitarian purposes came to craft a formal data protection approach. Thus, it is notable that both the ICRC and UNHCR rules/policy are broadly phrased, that UNHCR policy as applicable to refugees and other persons of concern explicitly references ensuring conformity with the UN Guidelines as a core purpose,[59] and that both the ICRC and UNHCR restrictions/derogations provisions clearly draw

58 This understanding of IOs' position in the area of data protection has clearly become dominant in the intervening period. See International Conference of Data Protection and Privacy Commissioners, "Resolution on Data Protection and International Organizations," (12 September 2023), https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-International-Organisations.pdf and Massimo Marelli, "The law and practice of international organisations' interaction with personal data protection regulation: At the crossroads between the international and domestic legal orders" *Computer Law & Security Review*, 50 (2023), https://doi.org/10.1016/j.clsr.2023.105849.

59 UNHCR, "Policy on the Protection of Personal Data of Persons of Concern to UNHCR," s. 1.1.

on the 'humanitarian clause' set out in the UN Guidelines.[60] The specific impact of the UN Guidelines on the regulation of non-governmental humanitarian IOs is less discernible. Given that these organisations are much more clearly subject to local law, this is perhaps unsurprising. Nevertheless, at least through influencing such local law, the understandings set out in the UN Guidelines have exerted an impact here also. Thus, following intervention by the ICRC in 2015,[61] a Recital to the EU GDPR explicitly recognises that "humanitarian purposes" can provide a ground for the restriction of general data protection provisions set out in that instrument[62] and, albeit only in highly restrictive circumstances, expressly confirms that transborder data transfers to "an international humanitarian organisation" may be justified as "necessary for an important reason of public interest or because it is in the vital interest of the data subject".[63] In short, although manifestly only 'soft' law, it is clear that even after thirty-five years the UN Guidelines remain a landmark normative text in relation to the data protection expectations applicable to international humanitarian organisations and that we can learn much from the individual and collective effort which led to this outcome.

60 UNHCR, "General Policy, s. 64; ICRC, "Rules," art. 14 (which explicitly references "ICRC's humanitarian mandate").

61 See Council of the EU, Document 7355/15 (25 March 2015), https://data.consilium.europa.eu/doc/document/ST-7355-2015-INIT/en/pdf and Council of EU, Document 8837/15 (12 May 2015), https://data.consilium.europa.eu/doc/document/ST-8837-2015-INIT/en/pdf.

62 GDPR 2016/679, Recital 73.

63 GDPR, Recital 112. Humanitarian purposes are also recognised in Recital 46 as potentially serving "both important grounds of public interest and the vital interests of the data subject". This more limited provision appears to have been suggested by Germany just prior to a general consideration of the ICRC's concerns. See Council of the EU, Document 17072/2/14 Rev 2, 11 (Recital 37a), https://data.consilium.europa.eu/doc/document/ST-17072-2014-REV-2/en/pdf.

9

LEGAL TENSIONS

Insights from UN-EU Correspondence on EU Data Protection Law and the Role of Privileges and Immunities in Enhancing Personal Data Protection

Christina Vasala Kokkinaki

Introduction

In today's era dominated by digital technology, the protection of personal data has become a priority for international organisations (IOs) as they increasingly adopt data-driven approaches that involve processing large amounts of personal data to enhance operational effectiveness and implement their respective mandates.[1] At the same time, States have granted IOs privileges and immunities to ensure their operational autonomy and independence when implementing their mandates globally.

Against this backdrop, this chapter examines the 2018–2024[2] correspondence between the United Nations' (UN) Legal Counsel (UNLC) on behalf of organisations in the UN system[3] ("the UN side"), and the European Commission (EC) and the European Data Protection Board (EDPB) ("the

1 See, for example, "Big Data for Sustainable Development," United Nations, https://www.un.org/en/global-issues/big-data-for-sustainable-development; Allard Buursma and John Karlsrud, "Predictive Peacekeeping: Strengthening Predictive Analysis in UN Peace Operations," *Stability International Journal of Security & Development*, vol. 9, no. 1 (2019), https://stabilityjournal.org/articles/10.5334/sta.663; and Ana Beduschi, "Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks," *International Review of the Red Cross*, No. 919, (2022), https://international-review.icrc.org/articles/harnessing-the-potential-of-artificial-intelligence-for-humanitarian-action-919.

2 At the time of writing, there has been no reply to the last letter dated 23 May 2024, available at: https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-under-secretary-general-legal-affairs-and-united_en.

3 The term "UN system organisations" is used in this chapter, as in the UN letters, to include the United Nations, its Funds, Programmes, and other subsidiary organs, as well as the UN Specialised Agencies and UN-related organisations.

DOI: 10.4324/9781003650164-14

EU side"). The correspondence was triggered due to the challenges posed to the activities of UN system organisations by the European Union's (EU) data protection legislation, particularly the General Data Protection Regulation[4] (GDPR) and the Data Protection Regulation for EU institutions[5] (EU DPR) which regulate, *inter alia*, the transfers of personal data to IOs. Initiated in 2018, just days before the GDPR took effect, the UNLC expressed concerns to the EU Delegation in New York about the GDPR's impact on the work of UN system organisations. One key issue stemmed from GDPR provisions regulating international data transfers (Chapter V), which made GDPR-subject entities hesitant to share personal data with UN system organisations, to the extent that, in some cases, they attempted to impose the GDPR on UN system organisations prior to transferring data. This created significant challenges, particularly for humanitarian organisations, as delays or even denials to share personal data hindered their ability to implement their mandate. Over six years, numerous letters were exchanged,[6] alongside in-person and remote meetings, in an effort to confer and attempt to find practical solutions.

According to the UN side, EU data protection law should not be directly or indirectly imposed on UN system organisations, which operate under the UN Charter, their own constitutive instruments, and mandates from member states. The handling of UN data by UN system organisations, as well as data transfers to them, should be unrestricted, based, *inter alia*, on the organisations' privileges and immunities, the special status of the UN under international law, and the pre-eminence of the UN Charter over any other international agreement binding on its members (including over EU Treaties). The UN side repeatedly requested the EU side to issue specific guidance to address the situation of the UN system organisations, aiming mainly at providing legal comfort to EU Member States and third parties subject to EU data protection law transferring data to or receiving data from UN system organisations. Conversely, the EU side maintained that EU data protection law requires the protection of the data to travel with the data, which is why Chapter V of the GDPR imposes specific conditions on entities transferring personal data to IOs. However, the EU side clarified that compliance with EU data protection law is the responsibility of the entities subject to it, and not

4 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies, and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC.

6 Many of the letters are publicly available on the EDPB website: https://www.edpb.europa.eu/our-work-tools/documents/letters_en.

the UN. Chapter V offers various tools for transfers, many of which work for transfers to IOs.

This chapter focuses on the UN's argumentation – while examining the EU side's response – that privileges and immunities not only ensure an organisation's independence but also enhance the protection of personal data. This is because they can successfully prevent forced disclosure of data and, thus, safeguard data from uses incompatible with the organisation's mandate, which is particularly important in the case of humanitarian organisations.

The UN's Privileges and Immunities Argumentation

The UN's position on privileges and immunities remained consistent over time, though its argumentation evolved. From its first letter in May 2018, the UN side emphasised its privileges and immunities, arguing that it is not subject to EU data protection law and that each UN system organisation applies its own policies for processing personal data. It specifically highlighted that the UN enjoys such legal capacity and such privileges and immunities in the territory of each of its Member States as necessary for the fulfilment of its purposes, as per Articles 104 and 105 of the UN Charter.[7] The UN side referenced key treaties elaborating its privileges and immunities, namely the Convention on the Privileges and Immunities of the United Nations[8] (the "1946 Convention"), the Convention on the Privileges and Immunities of the United Nations Specialized Agencies[9] (the "1947 Convention"), and other relevant multilateral and bilateral agreements,[10] while highlighting that all EU Member States are States Parties to the United Nations Charter, the 1946 Convention, and the 1947 Convention. It also raised concerns that certain entities were seeking to impose EU data protection law provisions on UN system organisations, despite their immunity from such legislation, particularly in cases involving data transfers to the UN. In early 2020,[11] the UN side elaborated further its position, arguing that UN "data" is part of the UN "archives" and "documents" and as such UN "property and assets"

7 United Nations, *Charter of the United Nations*, 1 UNTS XVI, 24 October 1945.

8 *Convention on the Privileges and Immunities of the United Nations* 1946, 1 UNTS 15.

9 *Convention on the Privileges and Immunities of the Specialized Agencies* 1947, 33 UNTS 261.

10 For example, the *Agreement on the Privileges and Immunities of the International Atomic Energy Agency*, IAEA Doc. INFCIRC/9/Rev. 1 (1959), 374 UNTS 148 (1960).

11 United Nations Secretariat, "Comments of the United Nations Secretariat on Behalf of the United Nations System Organizations on the 'Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies," 2020, 14–15, https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf.

covered by Article II of the 1946 Convention.[12] Therefore, UN data "wherever located" and "by whomsoever held" is immune from any form of interference, whether by executive, administrative, judicial, or legislative action.[13] UN data is also immune from every form of legal process, and is inviolable "wherever located".[14] Based on those three "types" of privileges and immunities, namely immunity from any form of interference, immunity from every form of legal process, and the inviolability of archives, the UN side concluded that insofar as EU data protection law sought to indirectly regulate the UN's handling of data or the transfers of data between the UN and its vendors or implementing partners, this would constitute legislative interference violating the obligations of UN Member States under the 1946 Convention[15] and Article 105 of the UN Charter.

The UN's argumentation in this respect appears well-grounded in light of the following points. Foremost, the overarching rationale of the UN's position is rooted in the very *raison-d'être* of privileges and immunities: the independent function of IOs across jurisdictions that ensures the fulfilment of their mandates without any obstacles.[16] States grant IOs privileges and immunities so that they can be independent in fulfilling their functions,[17] something that "could otherwise be compromised by unwanted interference from the host state".[18] Member States may not "hinder in any way the working of the Organization or take any measures the effect of which might be to

12 Data as "assets" is the approach that the ICRC took in its recent headquarters agreement with Luxembourg. See Andrea Raab-Gray and Massimo Marelli, "Inviolability in the digital era: The ICRC's Agreement on Privileges and Immunities with Luxembourg," *International Review of the Red Cross*, 2025, 15–17, https://doi.org/10.1017/S1816383125000190.

13 Article II, Section 3 of the 1946 Convention.

14 Article II, Sections 2 and 4 of the 1946 Convention.

15 The language of the 1946 Convention is mirrored in the 1947 Convention, so both of them are relevant to this argumentation.

16 See examples of caselaw confirming the independent functioning of the UN: *Manderlier v. Organisation des Nations Unies et l'Etat Belge*, Brussels Civil Court, 11 May 1966, JT 721 and *Broadbent et al v Organization of American States et al*, 628 F.2d 27, DC Cir., 8 January 1980, United States Court of Appeals.

17 Chittharanjan Felix Amerasinghe, "Privileges and immunities," *Principles of the Institutional Law of International Organizations*, (Cambridge University Press, 2005): 315–351. On the functionalism of international organisations see Jan Klabbers "Privileges and Immunities," *An Introduction to International Institutional Law*, (Cambridge University Press, 2002): 146–168. On the principles of functionality and independence, see Massimo Marelli, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders," *Computer Law and Security Review*, September 2023, 5, https://www.sciencedirect.com/science/article/pii/S0267364923000596.

18 Eric De Brabandere, "Measures of Constraint and the Immunity of International Organisations," *Immunity from Execution of States and International Organisations*, eds. Tom Ruys, Nicolas Angelet, and Luca Ferro, (Cambridge University Press, 2019): 211.

increase its burdens, financial or other", as per the report of the drafting committee of the 1946 Convention.[19] Arguably, indirect regulation of the UN's handling of personal data constitutes such a burden. Moreover, the fact that all EU Member States are parties to the 1946 and the 1947 Conventions adds additional weight to the UN's position,[20] as it emphasises the legal obligation of all EU Member States to respect, *inter alia*, the UN's immunity from legal process, immunity from any form of interference, and the inviolability of its archives. Lastly, as the UN side pointed out, the language used for immunity from any form of legal process in the 1946 and 1947 Conventions clarifies that immunity is applied to property and assets no matter where they are located and no matter who holds them.[21] Therefore, UN data (as part of "property and assets") cannot be interfered with, even if it is not located within the UN premises and even if it is not held by the UN itself. The UN's argument effectively highlights how the broad scope of immunity protects its data from external interference.

The UN side chose not to analyse in depth its privileges and immunities' argumentation. For example, there was no detailed explanation of the terms "immunity" and "inviolability",[22] nor an analysis of "immunity from every form of legal process" when concluding that the UN is immune from legislation and that the GDPR is not applicable to it. In the context of the specific correspondence, there was no need to do that, especially given the broad interpretation of the UN's privileges and immunities under jurisprudence[23]

19 Division of Immunities and Treaties of the Legal Document, *Handbook on the legal status, privileges and immunities of the United Nations*, ST/LEG/2, 19 September 1952, 22.

20 At the same time, it can also be argued that it is "awkward" for the UN to have to rely on the individual obligations of EU Member States instead of those of the EU itself. See Fernando Lusa Bordin, "Is the EU Engaging in Impermissible Indirect Regulation of UN Action? Controversies over the General Data Protection Regulation," *EJIL: Talk!*, 11 December 2020, https://www.ejiltalk.org/is-the-eu-engaging-in-impermissible-indirect-regulation-of-un-action-controversies-over-the-general-data-protection-regulation/.

21 Article II, Section 3 of the 1946 Convention: "The property and assets of the United Nations, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action". This language is mirrored in the 1947 Convention.

22 Noting that some scholars argue that "inviolability" is a more appropriate term compared to "immunity", because inviolability contains a positive obligation to protect the object of inviolability by not interfering with it, and it is not necessarily linked to legal proceedings. See Raab-Gray and Marelli, "The ICRC's Agreement with Luxembourg," 9.

23 Examples of case law include *Manderlier v. Organisation des Nations Unies et l'Etat Belge*, 1966, *Broadbent et al v Organization of American States et al*, 1980, *Spaans v. Iran-United States Claims Tribunal*, Final appeal judgment, Case No 12627, Decision No LJN: AC9158, NJ 1986, 438, (1987) 18 NYIL 357, ILDC 1759 (NL 1985), 20 December 1985, Supreme Court, Netherlands, 1983.

and academic writings.[24] Both the 1946 and 1947 Conventions establish an "undefined and unrestricted"[25] immunity from legal process that encompasses jurisdictional immunity (immunity from suit) and immunity from execution measures, granting (i) the UN and (ii) UN property and assets absolute[26] immunity from all legal actions. This interpretation of absolute[27] immunity remains widely accepted.[28] Additionally, distinguishing the "application" of the law from "enforcement" would not serve any purpose in the correspondence, especially since the EU side stated early on that the GDPR is not applicable to UN system organisations.[29] With that matter resolved, the UN side refined its privileges and immunities' argumentation, shifting from asserting the non-applicability of EU data protection law to emphasising the legislative interference such law poses to UN activities. The issue of "application" or otherwise of EU data protection law to IOs, as distinct from

24 For example, August Reinisch, "Introduction to the General Convention," in *The Conventions on the Privileges and Immunities of the United Nations and its Specialized Agencies: A Commentary*, ed. August Reinisch, 2016, online ed., Oxford Academic, https://doi.org/10.1093/law/9780198744610.003.0001 and Amerasinghe, "Privileges and immunities".

25 Reinisch, "Introduction to the General Convention," 5.

26 On the distinction between absolute and functional immunity, Reinisch argues that "judicial practice in several jurisdictions shows that the application of 'absolute' or 'functional' immunity usually largely leads to the same scope of immunity, i.e. absolute or quasi-absolute immunity, because any activity of an international organization, other than one performed *ultra vires*, can be understood as functionally necessary, given the delegated nature of international organizations' powers". See August Reinisch and Gregor Novak, "International Organizations," *International Law in Domestic Courts: A Casebook*, eds. André Nollkaemper et al., 2018, online ed., Oxford Academic, 177–178, https://doi.org/10.1093/law/9780198739746.003.0005.

27 Nowadays, the Court's perspective in the Manderlier case characterising the UN's immunity as absolute remains valid. See Pierre Schmitt, "Manderlier v Organisation des Nations Unies and Etat Belge," *Judicial Decisions on the Law of International Organizations*, eds. Cedric Ryngaert et al., 2016, online ed., Oxford Academic, 374, https://doi.org/10.1093/law/9780198743620.003.0040. For an analysis of case law of national courts concerning the United Nations' immunity from legal process, see Jan Wouters and Pierre Schmitt, "Challenging Acts of Other United Nations' Organs, Subsidiary Organs, and Officials," *Challenging Acts of International Organizations Before National Courts*, ed. August Reinisch, online ed., Oxford Academic, 2010, https://doi.org/10.1093/acprof:oso/9780199595297.003.0004.

28 August Reinisch, "Immunity of Property, Funds, and Assets (Article II Section 2 General Convention)," *The Conventions on the Privileges and Immunities of the United Nations and its Specialized Agencies: A Commentary*, ed. August Reinisch, online ed., Oxford Academic, 2016, https://doi.org/10.1093/law/9780198744610.003.0006. About how absolute immunity has sometimes been characterised as anachronistic, but is essential in order to allow the organisation to implement its functions effectively and independently, see Eric De Brabandere, "Immunity of International Organizations in Post-Conflict International Administrations," *International Organizations Law Review*, vol. 7, no. 1 (2010): 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1993000.

29 See *infra*, "The EU side's response to the UN's privileges and immunities argumentation".

its "enforcement", has recently been addressed by scholars,[30] however this was not a contentious point in the UN-EU correspondence.

The EU Side's Response to the UN's Privileges and Immunities' Argumentation

The EU side did not dispute the UN's privileges and immunities. This merits attention because the EU itself, as an organisation with its own legal personality, is not a party to the UN Charter, or to any of the treaties granting the UN privileges and immunities.[31] In fact, in one of its early letters of July 2018, the EU side noted that UN privileges and immunities imply that EU rules are not, as such, applicable to the UN, even if UN offices may be located in the territory of an EU Member State. It further elaborated that it would be incorrect to state that the GDPR would apply to UN entities, as this would be a violation of their privileges and immunities. This gives the impression that for the EU side, the GDPR is not "applicable" to IOs, or UN system organisations at a minimum. In later correspondence in December 2019, the EU side reformulated its position and stated that in light of the clarification provided by the EDPB territorial scope guidelines[32] "the GDPR *applies* with full respect for the privileges and immunities of international organisations such as the UN" (emphasis added). Following that, the UN consistently reaffirmed the EU's initial statement confirming the "non-applicability" of the GDPR to UN system organisations, leading the EU's later reformulated statement to fade from focus. In practice, no matter the debate in the academic sphere

30 For example, Christopher Kuner notes that the application of the GDPR to international organisations cannot be automatically excluded because (i) the data processing activities of international organisations often fall under the GDPR's material and territorial scope, and (ii) the scope of the privileges and immunities of international organisations varies. See Christopher Kuner, "International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between the EU law and International Law," 16 IOLR 171, 27, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3050675. Marelli argues that there is a "pragmatic arrangement" between the international and the domestic legal orders that results in the latter indirectly acknowledging that IOs are not expected to apply the rules of the domestic legal order. See Marelli, "International organizations' interactions with personal data protection domestic regulation", 16. Saab-Gray and Marelli further elaborate that the non-application of the law is grounded on archive inviolability, encompassing a protection from State interference, including by legal process. See Raab-Gray and Marelli, "The ICRC's Agreement with Luxembourg," 9.

31 On this point, Kuner notes that "The CJEU has not yet issued a clear pronouncement on the status of privileges and immunities of IOs with respect to EU law. However, there are several theories under which it could be argued that those granted to IOs by the Member States should be binding on the EU as well". See Kuner, "International Organizations and the EU GDPR," 19.

32 European Data Protection Board, "Guidelines 3/2018 on the Territorial Scope of GDPR (Article 3)," 2019.

mentioned earlier, no EU court has decided that an IO is expected to apply EU data protection law.

Interestingly, the EU side did not address in detail the UN's privileges and immunities' argumentation, including the argument that EU data protection law interferes with the data handled by UN system organisations. It highlighted, however, that Articles 104 and 105 of the UN Charter do not create a positive "right to obtain personal data" and it reiterated multiple times that the protection offered by EU data protection law needs to travel with the data. It is difficult not to view this "travelling" of the protection as interference, albeit arguably a positive one, as it does indeed require UN system organisations receiving personal data under Chapter V of the GDPR to uphold a certain standard when handling such data, so that the protection has indeed "travelled". Even if the onus is with the entity transferring the data to ensure that Chapter V conditions are applied, this may lead in practice to such an entity refusing to transfer data to a UN system organisation because of its assessment that the Chapter V conditions cannot be applied. On this point, it could be argued that the UN raised its concerns about the GDPR interference too late, given that the law was already in effect. Such concerns could have been highlighted during the GDPR's drafting stage[33] resulting potentially in a different GDPR text to alleviate any legal tensions.[34] However, monitoring global legislative developments is not the UN's role; it is the responsibility of States to ensure that the privileges and immunities they have committed to grant organisations under international treaties are respected and upheld. As it stands, the GDPR's legal text lacks interpretative flexibility to provide the UN side the legal comfort it requires.[35] It can only be assumed that the drafters included certain provisions not to enforce binding compliance but to

33 The UN side specifically noted in this respect that "Had input from the United Nations been solicited during the development of the General Data Protection Regulation, the pertinent differences between States and the United Nations would have been remarked (among other issues)". See United Nations Secretariat, "Comments of the United Nations Secretariat on the Guidelines 2/2020," 10.

34 An organisation that expressed its views during the drafting process is the ICRC. This contributed to the formulation of Recital 112 of the GDPR as follows: "Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject".

35 There is only one recent article arguing that the text of the GDPR allows for an interpretation under which derogations under the GDPR provide the most viable avenue for data transfers to international organisations. See Massimo Marelli, "Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms," *International Data Privacy Law*, vol. 14, no. 1 (2024): 19–36, https://doi.org/10.1093/idpl/ipad022.

nudge IOs towards adopting stronger data protection policies, thus aligning with EU standards.[36]

The Outcomes of the Correspondence

The UN-EU correspondence led to several concrete outcomes, some of which arguably eased the challenges posed by EU data protection law to the work of UN system organisations.

Firstly, three sets of EDPB guidelines[37] ultimately incorporated provisions relevant for IOs: they clarified that the application of the GDPR is without prejudice to the provisions of international law on the privileges and immunities of IOs;[38] they referred to IOs having their own internal rules/regulatory framework;[39] they explained that transfers to IOs must be in compliance with international law and without prejudice to privileges and immunities;[40] and they clarified that for transfers to IOs, the oversight body need not be external but must function independently with binding decisions.[41] The above clarifications could be viewed as an informal recognition of the privileges and immunities of IOs, as the EDPB advocates interpreting specific GDPR provisions in light of such privileges and immunities. Kuner[42] observed as early as 2018 that exactly this approach can alleviate the tension between the GDPR and instruments of international law that grant privileges and immunities.

Secondly, a taskforce was created to facilitate informal discussions on the issue of transfers of personal data to IOs. It was led by the European Data Protection Supervisor and gathered representatives from IOs, the European Commission, EU Data Protection Authorities, and data protection officers of EU institutions. The taskforce developed a template for transfers between

36 See Bordin, who, when comparing the GDPR situation with the Kadi judgment, states that "There can be benefits, of course, in the kind of 'peer review' of UN action that the EU has proved capable of conducting. *Kadi* was, after all, the catalyser of much needed reform in the delisting process at the Security Council". Bordin, "Is the EU Engaging in Impermissible Indirect Regulation?", 2020.

37 "Guidelines 3/2018 on the Territorial Scope of GDPR (Article 3)," 2019, 23. "Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies," 2020. "Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR," 2023, 7. Whereas the Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, which were adopted prior to the UN-EU correspondence, do not refer to the privileges and immunities of international organisations.

38 "Guidelines 3/2018 on territorial scope," 23.

39 "Guidelines on transfers," 43.

40 "Guidelines on transfers," 47.

41 "Guidelines on transfers," 63.

42 Kuner, "International Organizations and the EU GDPR," 29.

EU institutions and IOs under the GDPR, discussing the comments of IOs on the draft template prepared by the EU side. Overall, even though the taskforce allowed for useful exchanges at a technical level, the UN considered that the finalisation of the template came unexpectedly and it fell short of its expectations.[43] The UN reiterated its "overall strong objection to the Model, which cannot form the basis of viable arrangements for transfers from European Union institutions to United Nations System Organizations unless it is significantly revised in each specific situation while allowing for all necessary flexibility".[44] It seems that the negotiations on the template reached an impasse, as despite the EU side's genuine efforts to incorporate the UN side's comments, the constraints[45] inherent in the law ultimately precluded any further flexibility.

Thirdly, numerous coordination meetings were held to address specific contractual negotiations pertaining to data transfers, with EU representatives constructively assisting in meetings between the UN side and entities subject to EU data protection law that were hesitant about transferring personal data to UN system organisations. Their involvement helped clarify complexities in the interpretation of the law in a manner that respected the privileges and immunities and overall status of UN system organisations. While not all the negotiations were successful, the approach contributed to raising awareness on the matter and facilitated transfers of data in many instances.

Lastly, and importantly, the UN's repeated requests to the EU side for a dedicated set of guidelines "addressing the situation"[46] of UN system organisations remained unmet.[47] This request was initially made to the European Commission, which presumably did not consider itself the appropriate body to issue such guidance. As for the EDPB, again presumably, if it had created such guidelines, it would have been the first time for it to address a specific type of

43 The UNLC stated in its letter of February 2024 that the final template "continues to seek to regulate onward transfers from international organizations and it continues to envisage oversight and redress mechanisms that are not compatible with the applicable international law, as well as the regulatory framework governing UN System Organizations, including the single audit principle", https://www.edpb.europa.eu/system/files/2024-08/letter-from-un-legal-counsel-edpb-chair_en.pdf.

44 UNLC Letter to EDPB, February 2024, 4.

45 For further analysis on the constraints of the law, on why adequacy and appropriate safeguards do not work well for transfers to international organisations, but derogations may, see Marelli, "Transferring personal data to international organizations," 19–36.

46 United Nations Secretariat, "Comments of the United Nations Secretariat on the Guidelines 2/2020," 25.

47 The request was made already in the first letter of the UN side to the EU side in May 2018. Throughout the correspondence, the UN side elaborated on what such guidance should entail. For the specific list of elements requested to be included in the guidelines, see United Nations Secretariat, "Comments of the United Nations Secretariat on the Guidelines 2/2020," 25–26.

entity (in this case, the UN). Most of the existing EDPB guidelines do not focus on specific industries, companies, or organisations; they are applicable across various sectors so as to promote consistency and fairness. The EDPB could potentially be accused of favouritism for treating a specific IO differently from all the others. The EDPB was particularly careful in its guidelines to address issues concerning IOs, and not to focus solely on the UN. Lastly, even if the EDPB considered that it had the authority to issue such guidelines, it would have been challenging to have a uniform approach for all UN system organisations, as they have varied mandates. EU data protection law, in addition, does not have specific provisions for UN system organisations compared to other IOs, despite the UN's unique universal character. This underscores the complexity of reconciling the UN side's request in line with its privileges and immunities and EU data protection requirements.

Exploring Privileges and Immunities as an Additional Data Protection Measure

As previously noted, the UN's argument rested on three "types" of privileges and immunities: immunity from every form of legal process, immunity from any form of interference with UN property and assets, and the inviolability of UN archives. Although not highlighted in the UN-EU correspondence, those privileges and immunities not only enable an IO to fulfil its mandate effectively and independently but also reinforce data protection by upholding its commitment to "purpose specification",[48] as elaborated further below.

At the outset, it is essential to bear in mind that a multitude of national laws allow governments to compel legal entities to disclose their data. For example, under Canada's Personal Information Protection and Electronic Documents Act[49] (PIPEDA), a government institution can request the disclosure of personal information without the knowledge or consent of the data subject if it suspects that the requested information relates to national security, the defence of Canada, or the conduct of international affairs. Usually, national laws requiring disclosure include provisions[50] that require warrants, court orders, or subpoenas that provide authorisation to governmental

48 The principle of purpose specification is embedded within international organisations' data protection frameworks. See, for example, UN Principles on Personal Data Protection and Privacy, 2018 https://unsceb.org/privacy-principles and ICRC Rules on Personal Data Protection, 2015, https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

49 See Section 7(3) (c.1) of PIPEDA, 2000.

50 See, for example, Section 7 (3) (c) of PIPEDA and the United Kingdom's (UK) Crime (Overseas Production Orders) Act, 2019, which allows UK investigatory and prosecution authorities to request a Crown Court to order a company based outside the UK to disclose information for it to be used in a criminal investigation or prosecution.

authorities to demand access to data. In the US, as another example, the Stored Communications Act[51] contains specific conditions under which governmental authorities can access electronic data stored by service providers subject to US jurisdiction.

The enforcement of such laws on IOs would be inconsistent with the privileges and immunities enjoyed by such organisations. Such national laws cannot be enforced on IOs, such as the UN, enjoying immunity from every form of legal process. Reinisch[52] clarifies that immunity from legal process for the UN comprises adjudicatory immunity, meaning that the UN is exempt from the adjudicatory jurisdiction of national courts. Thus, a national court would, in principle, not have jurisdiction to adjudicate on a case concerning compelled disclosure from the UN. Another important point to consider is that it would be contrary to the immunity from any form of interference if such national laws were to compel disclosure by IOs. For the UN, as per Bartholomeusz,[53] interference can take many forms, such as a conflict between the UN's procurement rules and the host State's binding procedures for contracts. However, not all governmental actions are forms of interference, and nowadays UN operations generally accept bureaucratic procedures as long as they do not cause significant delays or result in denials of entry. Given this, compelled disclosure appears indeed to constitute a form of interference, thus violating Article II, Section 3 of the 1946 Convention.

A final consideration concerns the inviolability of archives, which, as Burci[54] usefully clarifies,

> aims at protecting records and information whose exclusion from public access and from the exercise of national jurisdiction is considered necessary for the proper exercise by the UN of its functions. *Third parties, including national authorities, cannot legally force the disclosure of such information* and can only gain access to it with the consent of the UN Secretary-General.

51 Stored Communications Act, 18 U.S.C, 1986, paras. 2701 et seq. In addition, the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018 allows US law enforcement authorities to request entities subject to it for data stored not only within the US but also overseas. See also "Privileges and immunities and the cloud," *Handbook on Data Protection in Humanitarian Action*, 166 and Raab-Gray and Marelli, "The ICRC's Agreement with Luxembourg," 23–24.

52 Reinisch, "Immunity of Property, Funds, and Assets," 65.

53 Lance Bartholomeusz, "Inviolability of Premises (Article II Section 3 General Convention)," *The Conventions on the Privileges and Immunities of the United Nations and its Specialized Agencies: A Commentary*, ed. August Reinisch, 2016, online ed., Oxford Academic, 135, https://doi.org/10.1093/law/9780198744610.003.0008.

54 Gian Luca Burci, "Inviolability of Archives (Article III Section 6 Specialized Agencies Convention)," *The Conventions on the Privileges and Immunities of the United Nations and its Specialized Agencies: A Commentary*, 166.

> In practice, inviolability does not constitute an absolute obstacle to the accessibility of information held by the UN but rather translates into the right of the latter to determine which categories of information should be considered sensitive or confidential and under which conditions, if any, it may be disclosed. (emphasis added)

Thus, inviolability specifically ensures that no third entity can legally compel the UN to disclose its documents. And given that personal data processed by UN system organisations would be contained, in one way or another, within UN documents, personal data processed by the UN cannot be forcibly disclosed.

Inviolability of archives is particularly important as it covers archives "wherever located", which demonstrates that the location of the documents is not relevant for the inviolability afforded to them. This means that UN documents are inviolable no matter if they are stored in UN premises[55] or elsewhere. Even though third parties, such as service providers[56] storing or otherwise processing UN data may not enjoy privileges and immunities themselves, UN data is still covered by inviolability. This is the case even if service providers store documents and data of IOs in cloud environments; they still enjoy protection under privileges and immunities.[57]

Why does forced disclosure by governmental authorities matter? Because governments may use personal data they receive through forced disclosure for a variety of purposes, many of which may be incompatible with the mandate of certain organisations, especially humanitarian ones. For example, governments may legally use personal data to forcibly deport migrants to their countries of origin. In a humanitarian context, governments may use data to identify and target minorities or deliberately block access to humanitarian assistance based on political, religious, or ethnic biases. Such uses of personal data would not take place – at least not intentionally – by an international humanitarian organisation. Humanitarian organisations process personal data to carry out their humanitarian mandate. In this respect, any processing of personal data by a humanitarian international organisation would not, in principle, be used for any purpose incompatible with the humanitarian nature of their work. Privileges and immunities can shield humanitarian organisations from data

55 Burci, "Inviolability of Archives," 175.

56 For further analysis of the phrase "wherever located" see Raab-Gray and Marelli, "The ICRC's Agreement with Luxembourg," 12–14.

57 For further analysis on the application of privileges and immunities in cloud-based environments, as this point will not be analysed in this chapter, see "Privileges and immunities and the cloud," Massimo Marelli ed., ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition, Cambridge, 2024, 166–167, https://doi.org/10.1017/9781009414630, and Raab-Gray and Marelli, "The ICRC's Agreement with Luxembourg," 23–24.

requests or compelled disclosures, reducing the risk of data being used for non-humanitarian purposes. Accordingly, they help ensure that humanitarian organisations uphold the principle of purpose specification by using personal data solely in ways aligned with their humanitarian mandate. Yet, for humanitarian organisations not enjoying privileges and immunities, the risk of authorities using data for non-humanitarian purposes can have a negative impact on data subjects, as highlighted by the 2015 International Conference of Privacy and Data Protection Commissioners' Resolution on Privacy and International Humanitarian Action.[58]

Are privileges and immunities as a way to prevent forced disclosure effective in practice? The small number of court cases concerning access to UN documentation indeed seems to confirm the view, as per Burci, that "the need to respect the UN's control over at least a core of its records and information necessary for the independent exercise of its functions still constitutes an effective legal protection enjoying a broad measure of acceptance by UN member States and other stakeholders".[59] Moreover, there is an abundance of case law where courts have indeed confirmed the absolute immunity of the UN, deciding that they did not have jurisdiction to adjudicate against the UN.[60]

Thus, the legal shield provided by privileges and immunities prevents governments from accessing personal data processed by IOs, and, as a result, further prevents them from using personal data for purposes misaligned with the organisations' mandates.

Conclusion

The UN-EU correspondence underlines the legal tensions between the UN's privileges and immunities and EU legislation, specifically in the area of data protection. Despite the mutual efforts to address such tensions, the overall unresolved issues of the correspondence demonstrate the need for continued dialogue and pragmatic solutions. Perhaps a greater emphasis on the role of privileges and immunities as an additional data protection measure could

58 37th International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, 27 October 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

59 Burci, "Inviolability of Archives," 177.

60 See *Manderlier v. Organisation des Nations Unies et l'Etat Belge*, 1966, *Broadbent et al v Organization of American States et al*, 1980, *Cynthia Brzak and Nasr Ishak v United Nations, Kofi Annan, Wendy Chamberlin, Ruud Lubbers, et al*, 551 F. Supp. 2d 313 (S.D.N.Y. 2008), 597 F.3d 107 (2d Cir 2010) and *Stichting Mothers of Srebrenica and others v Netherlands and United Nations*, Netherlands, Supreme Court, Final appeal judgment, 13 April 2012, LJN: BW1999; ILDC 1760 (NL 2012).

move the discussions forward, as privileges and immunities could be framed not merely as legal shields for independence but also as mechanisms contributing to the protection of data. Emphasising this role could help shift the focus of the negotiations away from legal tensions and jurisdictional incompatibilities towards the shared goal of protecting personal data while respecting international law.

10

THE COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA (CONVENTION 108+) AND INTERNATIONAL ORGANISATIONS

Jean-Philippe Walter and Sophie Kwasny[1]

Introduction

The Council of Europe has played a pioneering role in the field of personal data protection. With the emergence of information and communication technologies, the Council of Europe has been concerned since the 1970s with the need to establish legal frameworks governing the processing of personal data, in order to ensure respect for human rights and individual freedoms. On 26 September 1973, the Committee of Ministers adopted Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, followed on 20 September 1974 by Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector. These two resolutions were the first step towards the adoption of a legally binding text.

On 17 September 1980, the Committee of Ministers of the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series No. 108), which was opened for signature on 28 January 1981. The Convention entered into force on 1 October 1985. It is the first and only binding international text on data protection of universal scope. The Convention has inspired numerous texts, and its similarities with the Guidelines for the Regulation of

1 The author was Head of the Data Protection Unit of the Council of Europe from 2011 to 2021. The opinions and views expressed in this chapter are the author's own and do not necessarily reflect those of the organisation.

DOI: 10.4324/9781003650164-15

Computerized Personal Data Files[2] adopted by the United Nations General Assembly on 14 December 1990 are particularly noteworthy. The Convention has been ratified by all 46 member states of the Council of Europe. Open to accession by non-member states of the Council of Europe, it has been joined by nine other countries to date.[3]

To mark the thirtieth anniversary of the opening for ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the Council of Europe and the Convention 108 Advisory Committee began the process of modernising this unique international legal instrument. The work culminated in the Committee of Ministers adopting the Protocol amending Convention 108 on 18 May 2018. The Protocol was opened for signature by the Parties on 10 October 2018. It will enter into force once it has been accepted by at least 38 States Parties,[4] and will apply only to those States that have ratified it.

While the provisions of the Convention and its additional Protocol regarding supervisory authorities and transborder data flows remain fully relevant to the processing of personal data, the necessary adjustments have been made to better meet the challenges posed by globalisation, interconnection, and digitalisation of society as a whole. Convention 108 was adopted at a time before the internet, smartphones, big data, social networking, and artificial intelligence (AI) were commonplace. Interest in personal data and threats to human rights and fundamental freedoms were not (yet) as widespread as they are today.

Convention 108 provides an excellent basis for meeting the legitimate expectations of data subjects and controllers, while strengthening the effectiveness of data protection and the implementation of its fundamental principles. As a preliminary point, it is worth recalling the main features of Convention 108 and its additional Protocol.

The Convention aims to reconcile the right to privacy and freedom of information, including the free flow of data regardless of frontiers – fundamental freedoms enshrined in Articles 8 and 10 of the European Convention on Human Rights.

The Convention is the reference text for numerous international and national texts, and the only binding international text regulating data protection. It sets out the basic, universally recognised principles of data protection, and its binding legal standards are fully consistent with other texts such as the

2 United Nations General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, United Nations General Assembly, New York, 1990, 3.

3 Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Russian Federation, Senegal, Tunisia, and Uruguay.

4 As of 2 June 2025, 33 States have ratified the amending protocol. See https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

various European Union (EU) data protection regulations, the Organisation for Economic Co-operation and Development (OECD) guidelines, and the United Nations (UN) guidelines.

The Convention is written in simple, general terms and follows a "technologically neutral" approach. It applies horizontally to all data processing operations in the private and public sectors, including in the areas of police, internal security, defence, and justice.

It guarantees a high level of protection in accordance with existing legal systems and in principle ensures the free circulation of data between State Parties, while requiring (through its additional Protocol) an adequate level of protection for transfers to recipients not subject to the Convention.

It governs cooperation between Parties and assistance to data subjects, regardless of their nationality or place of residence. It sets up a platform for multilateral cooperation through the Advisory Committee.

Finally, it is essential to note that the Convention is not intended to be applied solely on the European continent and is open to accession by States from other parts of the world, giving it universal potential.

Between 2011 and 2018, the Council of Europe, through the work of different committees, carried out the modernisation of the Convention to better adapt it to identified and emerging needs.

Objectives of the Modernisation

Adopted on 18 May 2018 by the Committee of Ministers of the Council of Europe in the form of a Protocol amending Convention 108, the modernised Convention, most commonly referred to as "Convention 108+", strengthens the rights of individuals and the obligations of controllers, while maintaining a technologically neutral approach that is legally compatible with other regulatory frameworks.

Several core objectives guided the modernisation exercise, which aimed at managing privacy challenges arising from the use of information and telecommunication technologies, while maintaining the general, technologically neutral nature of the Convention's provisions, and strengthening the right to data protection as a fundamental right essential to the exercise of other rights and fundamental freedoms when processing personal data.

The modernised Convention aims at increasing individuals' control over the data concerning them, and ensuring respect for human dignity when processing personal data. It also strives to reconcile the right to data protection with the exercise of other fundamental rights and freedoms, particularly the freedom of expression.

Finally, the modernisation strengthens the Convention's implementation and monitoring mechanisms and aims to ensure consistency and compatibility with the EU legal framework.

Convention 108+ preserves, reaffirms, strengthens, and promotes the universal vocation and open character of the Convention.

In order to match those multiple objectives, a thorough review and upgrade of the existing provisions was undertaken, which translated into important novelties being introduced throughout the Convention as detailed below.

Main Features of Convention 108+

With the modernisation of Convention 108, its original principles have been reaffirmed, some have been strengthened, and some new safeguards have been laid down. They had to be applied to the new realities of the online world while new practices had led to the recognition of new principles in the field. The principles of transparency, proportionality, accountability, data minimisation, privacy-by-design, etc. are now acknowledged as key elements of the protection mechanism and have been integrated into the modernised instrument.

Object and Purpose

In its preamble, Convention 108+ stresses the absolute need to "secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data".[5]

Article 1 sets out the aim of the Convention, namely "to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy".[6] With this wording, the Convention does not create a hierarchy of rights, but emphasises that the processing of personal data affects other rights and fundamental freedoms, and that respect for them requires the right to data protection to be guaranteed. The right to data protection is related to all other human rights and fundamental freedoms, and in fact strengthens them. In accordance with the principle of proportionality, this right must not be exercised in such a way as to prevent the exercise of other fundamental rights and freedoms. The aim is to reconcile the various rights and freedoms involved.

5 Convention 108+, Preamble, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

6 Convention 108+, Article 1.

Scope and Definitions

Convention 108+ applies not only to the automated processing of personal data, but to all (including non-automated) processing subject to a Party's jurisdiction in the private and public sectors. It therefore concerns manual processing, insofar as the data forms part of a set the structure of which makes it possible to search for data by data subject, according to specific criteria. The expression "subject to its jurisdiction" enables the Convention to "better [stand] the test of time and [accommodate] continual technological developments".[7] Although not expressly mentioned, it must also cover processing arising from activities and services intended for individuals subject to the jurisdiction of a Party, and processing arising from the observation of the behaviour of data subjects taking place within the jurisdiction of a Party, even if such processing is operated by controllers not subject to the jurisdiction of a Party.

However, the Convention does not apply to data processing carried out by an individual to exercise exclusively personal or household activities. In this context, particular attention should be paid to the phenomenon of social networks and other internet services where personal information is shared in the course of purely household activities. While the delimitation criteria are difficult to establish, the Convention must be fully applicable whenever personal data is accessible to people outside the personal or household sphere. The exception does not apply to controllers or processors who provide the means to process personal data for such personal or household activities.

With regard to definitions, they have been refined. The definition of personal data has not changed and is based on the short definition provided in Convention 108. However, the Explanatory Memorandum clarifies the notion of an "identifiable" individual.[8] An individual is not identifiable if such identification requires unreasonable time or activities for the controller, or for any individual from whom the controller could reasonably obtain the identification. The term "identifiable" refers not only to the elements of an individual's civil or legal identity, but also to what makes it possible to distinguish one person from others.

In addition, the notion of "file" has been abandoned. The term "controller of the file" has been replaced by the term "controller", which will be supplemented by the terms "processor" and "data recipient". Unlike the General Data Protection Regulation (GDPR) of the EU, the definitions of genetic and biometric data have not been retained on the grounds that these notions are evolving and it is therefore premature to set them down in a legal text. The

7 Convention 108+, Explanatory report, para. 26.
8 Convention 108+, Explanatory report, para. 17.

explanatory report under Article 6 nevertheless clarifies the notions of genetic and biometric data.[9]

Duties of the Parties

The Convention is not directly applicable. Under the terms of Article 4, each Party shall take the necessary measures in its domestic law to give effect to the provisions of the Convention and secure their effective application. It is important to note that international organisations (IOs) can be parties to the Convention. The measures must enter into force at the time of ratification or accession to the Convention at the latest. In the current framework, there is no control over the Convention's implementation. In the future, the Convention Committee may evaluate the effectiveness of measures taken by a State or an IO to give effect to the provisions of the Convention. The Parties must actively contribute to this assessment.

Basic Principles

With respect to the basic principles of data protection, the current principles set out in Article 5 of Convention 108 are in themselves sufficient to cover the various situations involving the processing of personal data. Nevertheless, Convention 108+ helps strengthen these principles by supplementing the principle of proportionality. This principle no longer focuses primarily on data, which must be adequate, relevant, and not excessive in relation to the purposes for which it is processed. The principle of proportionality must also apply to processing, and in particular to the choice of means and methods of processing. Processing must therefore be proportionate, i.e. suitable and necessary to achieve the legitimate purpose being pursued, and should reflect a fair balance between the public or private interests and the fundamental rights and freedoms at stake. It must be respected at all stages of processing, "including at the initial stage, i.e. when deciding whether or not to carry out the processing".[10]

At present, the Convention does not set out any grounds for processing. It simply states in general terms that all data processing must be lawful. Convention 108+ introduces a new provision in Article 5.2 stipulating that data may only be processed if the data subject has given free, specific, informed, and unambiguous consent, or if the processing is based on a legitimate basis laid down by law. Such a legitimate basis may be based on domestic law, a prevailing legitimate public or private interest, or compliance with a

9 Convention 108+, Explanatory report, paras. 57 and 58.
10 Convention 108+, Explanatory report, para. 40.

legal obligation or contractual obligation binding the data subject. In order to preserve the flexibility and general nature of the Convention, unlike Article 6 of the GDPR, it does not specify the grounds for legitimising the processing in detail. Consent, where it is required, must be unambiguous, whatever the nature of the data processed. This strengthening is justified as it seems necessary, particularly in the virtual world, to dispel any ambiguity as to the validity of the consent expressed. This is particularly important in processing operations carried out online. Finally, it must be possible to withdraw consent within the limits of the principle of good faith.

Special Categories of Data (Sensitive Data)

With regard to sensitive data, Article 6 retains the principle of prohibiting processing in the absence of appropriate safeguards under domestic law supplementing those of Convention 108+. "Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination".[11] The catalogue of sensitive data has been expanded to include genetic and biometric data, data relating to trade union membership and, in addition to criminal convictions, data relating to offences and other criminal measures. The provision also distinguishes between data that is sensitive by nature (e.g. health data, genetic data) and data that becomes sensitive as a result of its use, such as data the processing of which reveals racial origin or political opinions. This second category focuses on the function of the processing. Thus, keeping a picture in a file is not necessarily sensitive if the aim of the processing is not to deduce information from analysis of the picture.[12]

Data Security

With regard to data security, Article 7.2 introduces the obligation for controllers to report data breaches. However, this obligation is limited to significant cases, i.e. breaches that may seriously interfere with the rights and fundamental freedoms of data subjects. At a minimum, the supervisory authorities shall be notified. At the time of notification, the controller must indicate the measures taken or planned to address the security breach.[13] Unlike the GDPR, Convention 108+ does not include an obligation to inform data subjects. However, the Explanatory Memorandum urges controllers to do so in the event of significant risks to the rights and freedoms of data subjects, "such

11 Convention 108+, Article 6.
12 Convention 108+, Explanatory report, para. 59.
13 Convention 108+, Explanatory report, para. 65.

as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage".[14] In addition, supervisory authorities may, within the scope of their powers, require controllers to inform data subjects. This solution leaves room to consider the particular circumstances of each situation.

Transparency of Processing

Article 8 of Convention 108+ regulates the obligation to guarantee the transparency of processing. The controller must provide[15] a minimum amount of information, particularly concerning their identity and habitual residence or establishment, the purposes of the processing they carry out, the recipients of the data, and the means of exercising the rights of the data subjects. If necessary, additional information must be provided to ensure fair data processing. This includes, for example, information on data preservation periods, knowledge of the reasoning underlying data processing, any transfers to third countries, and whether data collection is mandatory or optional. Contrary to EU law, and in keeping with the general nature of the Convention, the provision does not specify the time at which information should be given. However, to enable individuals to act in full knowledge of the facts and to assert their rights or give valid consent when required, information must be provided as soon as possible – either at the time of data collection or, if the data is not collected from the data subjects, at the time of their registration or within a reasonable period, but at the latest at the time of their first communication. The way in which information is provided will thus depend on the circumstances of the processing; the information will be given in a reasonable manner. In particular, there is no need to provide information if the individual is already in possession of it and the circumstances of the processing have not changed. The controller will not be obliged to provide this information where it is (materially or legally) impossible to do so or would involve disproportionate effort. Exceptions to the duty to inform are also possible under the conditions set out in Article 11 of the Convention, including on grounds related to the protection of national security, or the prevention and suppression of criminal offences.

14 Convention 108+, Explanatory report, para. 66.
15 Convention 108+, Explanatory report, para. 68.

Rights of Data Subjects

The rights of data subjects have also been strengthened, to increase individuals' control of their data and to ensure respect for the right to human dignity and non-discrimination.

It is important to highlight, as is the case for other core provisions of the Convention, that they may have to be articulated with other applicable legal frameworks. For instance, depending on the jurisdiction and circumstances of the case, Article 8 on the right to respect of private life of the European Convention on Human Rights will be fully relevant, as well as the EU legal framework.

Convention 108+ acts as a bridge between national and international data protection frameworks. It reinforces fundamental rights under the European Convention on Human Rights (ECHR) and offers a treaty-based complement to the GDPR, particularly valuable for global convergence. Strengthening the Convention's monitoring mechanisms and fostering political commitment among parties are essential for ensuring its practical effectiveness and enforcement alignment with other applicable legal frameworks.

With regard to the right of access, Article 9 extends the catalogue of information to be sent to the data subject when they exercise this right. In addition to the information that the controller must provide in light of transparency and the duty to inform, they must also provide information on the data's origin. In addition, the data subject shall be entitled to be informed of the reasoning underlying processing with results that are imposed on or applied to them. This new right is particularly important when using algorithms for automated decision-making,[16] especially when profiling individuals.[17] It is to be linked with another new right: that of not being subject to a decision significantly affecting the data subject or producing legal effects with regard to them, when this decision is taken solely on the basis of automated data processing, without the data subject being able to put forward their point of view and arguments. "In particular, the data subject should have the possibility to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that will have an impact on the result of the automated decision".[18] This right does not apply if the decision is authorised by a law that provides for appropriate measures to safeguard the rights, freedoms, and legitimate interests of the data subject.

16 Convention 108+, Explanatory report, para. 77.

17 For more on this, see https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680 5cdd00%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}.

18 Convention 108+, Explanatory report, para. 75.

Article 9 also expressly introduces a right for an individual to object at any time, on legitimate grounds, to the processing of personal data concerning them. However, the Convention does not expressly provide for a right to be forgotten, specifically a right to be forgotten digitally. Existing safeguards (data preservation period, right to rectification or erasure of data) combined with the right to object should offer sufficient protection.

Exceptions and Restrictions

The rights of the data subjects are not absolute, and under Article 11 of the Convention, they may be restricted where this is provided for by law, the essence of the fundamental rights and freedoms is respected, and the restriction constitutes a necessary and proportionate measure in a democratic society for:[19]

- the protection of national security, public safety, important economic and financial interests of the state, or the prevention and prosecution of criminal offences;
- the protection of the data subject and the rights and freedoms of others, notably freedom of expression and information. Also covered are the secrecy of communications, as well as business secrets, trade secrets, and other secrets protected by law.

Exceptions may also be made for the processing of data used for statistical or scientific research purposes, provided that there is no apparent risk of interfering with the rights and freedoms of data subjects. Finally, the derogations under Article 11 apply not only to the exercise of data subjects' rights, but also to certain basic principles of Article 5.4, notification of data breaches, and the duty to inform. In addition, in matters of national defence and security, derogations may also be made regarding the assessment of measures taken to give effect to Convention 108+ and to certain powers of the supervisory authorities, given that effective independent control and supervision are provided for.

Such derogations must be exceptional in nature and their necessity shall be examined on a case-by-case basis.[20] A measure must therefore "be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and adequate. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed".[21]

19 Convention 108+, Explanatory report, paras. 91 ff.
20 Convention 108+, Explanatory report, para. 93.
21 Convention 108+, Explanatory report, para. 91.

Obligations Concerning Data Protection

Convention 108+ also strengthens the responsibilities of those who process data or have it processed. Article 10 thus establishes the principle that the controller is responsible for respecting the right to data protection during all phases of processing, and for taking all appropriate measures – including in the case of subcontracting – to implement data protection provisions. The controller must also be able to demonstrate their compliance with the provisions of the Convention. This responsibility also covers the choice of means used for processing. In particular, the controller must use technologies that ensure rights and fundamental freedoms are upheld. The Article also introduces the obligation of the controller or processor to carry out an analysis of the potential impact of the planned processing on the rights and freedoms of individuals. The controller must design data processing operations in such a way as to prevent, or at least minimise, risks of breaching data protection law. They must establish internal mechanisms to demonstrate to data subjects and data protection authorities that processing operations comply with the data protection provisions applicable to them. These measures include, in particular, the appointment of a data protection officer.

These obligations, and particularly the impact analysis that must be considered for any processing of personal data, must be proportionate to the risks to the interests, rights, and fundamental freedoms of the data subjects. They may be adjusted according to the size of the company, the volume of data processed, its sensitivity, the nature, scope, and purpose of the processing,[22] the technologies used, and the risks that such processing may entail for data subjects.

Finally, these obligations should be interpreted as including the requirement that products and services intended for the processing of personal data and distributed on or from the jurisdiction of a Party incorporate easy-to-use features, making it possible to ensure that data processing complies with applicable law.

Transborder Data Flows

With regard to transborder data flows, Article 14 is based on the notion of an appropriate level of protection. The principle of the free flow of data between Parties to the Convention is maintained. It assumes an adequate level of data protection once a State or IO has ratified or acceded to the Convention, provided that the rights and obligations arising from the Convention have been effectively implemented. When necessary, the Convention Committee may

22 Convention 108+, Explanatory report, para. 90.

find the level of protection to be insufficient. A Party may, in certain cases, limit or even prohibit a transfer where there is a real and serious risk that the transfer will lead to circumvention of the Convention's provisions, or where it is required to comply with harmonised rules of protection shared by States belonging to a regional IO, such as the rules of the EU.

When the recipient does not come under the jurisdiction of a Party to the Convention, the transfer may, as a general rule, "only take place where an appropriate level of protection based on the provisions of the Convention is secured".[23] This level of adequacy can be ensured by the law governing the recipient, such as the existence of data protection legislation. It may result from standardised or *ad hoc* legal measures such as contractual clauses,[24] internal rules, or similar measures that are binding, effective, and capable of being effectively enforced, implemented by the individual communicating the data or making it accessible, or by the recipient. Data protection authorities shall be informed of the measures taken. They may require proof of the effectiveness and quality of these measures. Where appropriate, they may suspend, prohibit, or place conditions on the transfer; they may also require a review of the measures governing it.

In the absence of an appropriate level of data protection, the communication or provision of data remains possible under certain conditions. The transfer may take place with the data subject's consent. They must have been informed in advance of the risks arising from the absence of appropriate safeguards. The transfer may also take place if the specific interests of the data subject so require, for example, to safeguard their vital interests. It may also be carried out if legitimate interests protected by law so require. This concerns in particular the interests referred to in Article 11 of the Convention. These include the need for police and judicial cooperation in criminal matters. Such transfers, in the absence of an appropriate level of protection, do not need to be carried out regularly, but rather to cover specific situations. The supervisory authority may also suspend, prohibit, or place conditions on this type of data communication or provision in the absence of an appropriate level of protection.

Parties may derogate by means of legislative measures from the provisions governing transborder data flows where such derogations constitute a necessary and proportionate measure in a democratic society for the protection of freedom of expression and information. Such derogations may prove necessary, particularly in the context of the online dissemination of data relating to the exercise of these two fundamental freedoms.

23 Convention 108+, Article 14.

24 See https://www.coe.int/en/web/data-protection/convention-108-committee-t-pd-.

The crucial questions in the context of transborder flows are how to determine the appropriate or adequate level, and how to converge and coordinate the adequacy procedure within the EU with the assessments to be carried out at the Council of Europe. The appeal of Convention 108+ for third countries or IOs will also depend on recognising its suitability for the free flow of information with EU member countries.

Supervisory Authorities

Convention 108+ addresses the issue of supervisory authorities, which must be established by the Parties and are an essential condition for ensuring the effectiveness of the right to data protection. "In order for data protection supervisory authorities to be able to provide for an appropriate remedy, they need to have effective powers and functions and enjoy genuine independence in the fulfilment of their duties. They are an essential component of the data protection supervisory system in a democratic society".[25]

Incorporating Article 1 of the additional Protocol, Article 15 of the Convention specifies and completes the catalogue of functions and powers of the authorities by providing – in addition to the powers of intervention, investigation, engaging in legal proceedings and bringing violations of data protection provisions to the attention of the judicial authorities – a duty to raise awareness, to inform, and to educate the actors involved (data subjects, controllers, processors, etc.). It also envisages the possibility for authorities to take decisions and impose penalties. In addition, these authorities must be consulted on any legislative or administrative proposals that provide for the processing of personal data. The Convention also specifies the independence that the supervisory authority must enjoy in the exercise of its tasks and powers. In particular, these authorities must not be subject to instructions from the appointing authorities or any other entity. They must have adequate human, technical, and financial resources, as well as the infrastructure to carry out their tasks and exercise their powers effectively. In order to ensure their activities are transparent, supervisory authorities are required to draft and periodically publish a report on the measures taken to apply the data protection provisions.[26] Finally, clarification has been provided on the processing of legal proceedings. The supervisory authority must not interfere with the independence of the judiciary and is therefore not competent for processing carried out by public bodies in the exercise of their judicial functions. It is, however, competent for other processing.

25 Convention 108+, Explanatory report, para. 117.
26 Convention 108+, Explanatory report, para. 131.

Article 17 also emphasises cooperation among supervisory authorities. They must cooperate to the extent necessary to carry out their tasks, in particular by exchanging information relating to processing carried out on their territory or concerning their law and administrative practices relating to data protection. Cooperation should also include coordination of their investigations or interventions, as well as conduct of joint actions. The Convention stipulates that supervisory authorities may form a network to facilitate this coordination. Cooperation between the Parties, as already provided for in Articles 13 ff. of the Convention, will be the responsibility of the supervisory authorities in the future. The same applies to helping individuals to exercise their rights.

Convention Committee

Convention 108 set up an Advisory Committee to facilitate or improve the Convention's application. This Committee plays a fundamental role in the Convention's interpretation, the exchange of information between the Parties, and the development of data protection law. Articles 22 ff. of Convention 108+ provide for the creation of a Convention Committee, with a strengthened role and powers, to replace the current Advisory Committee. It will no longer be merely consultative, but will also have evaluation and monitoring powers. It "will have a key role in assessing compliance with the Convention".[27] In particular, it may issue opinions prior to accession to the Convention on the level of data protection offered by the State or IO concerned. It may also assess the conformity of the rules of domestic law governing this Party and verify the effectiveness of the measures taken (such as the existence of a supervisory authority or effective remedies or powers), especially to check whether the level of protection complies with the Convention's provisions. It will be able to assess whether the legal standards governing the transfer of data offer sufficient safeguards to ensure an appropriate level of data protection. It may develop or approve models of standardised safeguards. In order to assess the level of suitability, it will have to lay down the examination procedure in its Rules of Procedure. It will be able to develop models of standardised legal measures. Finally, it will play a facilitating role in the amicable resolution of difficulties arising in the Convention's application.

Pending the entry into force of Convention 108+ and the establishment of the Convention Committee, the current Advisory Committee is already developing various instruments in the form of interpretative opinions or

27 Convention 108+, Explanatory report, para. 162.

guidelines based on Convention 108+; these should facilitate the application of the new Convention.[28]

The Role of International Organisations

During the work to modernise Convention 108, the Advisory Committee involved observers from the private and public sectors, including representatives from non-governmental organisations and IOs, such as the International Committee of the Red Cross (ICRC), which contributed to the modernisation work as early as 2011. While the EU played an important role in negotiating the amending protocol, particularly to ensure perfect harmony with its regulations, the other IOs involved in the exercise also made a significant contribution. In particular, the ICRC has contributed to ensuring that the provisions of the Convention – while guaranteeing a high level of data protection – do not jeopardise the activities of these IOs, particularly in the humanitarian field, which requires processing of particularly sensitive personal data. The ICRC has also made it possible to consider the issue of data transfers for humanitarian purposes. This involvement of IOs in the Council of Europe's work is to be welcomed, since it helps to promote the Convention universally (as Interpol did with the 1981 Convention even before States applied it), to establish the right to protection of personal data in more distant parts of the world, and to ensure that this right evolves in light of the use of new technologies and new issues.

The Importance of Convention 108+ for International Organisations

The revision of Convention 108, resulting in Convention 108+, marked a major turning point for IOs, notably by paving the way for their formal accession. For the first time, Convention 108+ recognises their essential role in the governance of personal data worldwide, as well as the fact that these actors process personal data in transnational, sensitive, or emergency contexts, without always benefiting from a harmonised framework.

Due to their special legal status, IOs may not be directly subject to national regulations, and Convention 108+ thus provides them with a unique and adaptable legal framework that respects their institutional autonomy while guaranteeing a high level of data protection.[29]

28 See https://www.coe.int/en/web/data-protection/resources.

29 Massimo Marelli, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", *Computer Law & Security Review*, vol. 50 (2023), https://doi.org/10.1016/j.clsr.2023.105849.

Article 27 of the modernised Convention explicitly provides for the possibility of Ios' accession. This provision reflects a strong political commitment to inclusiveness and universality, which distinguishes Convention 108+ from other international instruments.

This role attributed to IOs was not limited to simple *ex post* legal openness (once Convention 108+ had entered into force): they were directly involved in the modernisation work, as observers and stakeholders on the Convention 108 Advisory Committee and the ad hoc Committee responsible for finalising the amending protocol.

This participation led to real collaboration in constructing standards, ensuring that the new provisions are both ambitious in terms of fundamental rights and realistic from an operational standpoint, with a view to normative convergence and clarification of the standards applicable to their operations.

The ICRC and Interpol were among the most active contributors, as each of them handle sensitive data.

Involved in the collection, processing, and storage of personal data in contexts of armed conflict and humanitarian crises, the ICRC emphasised the need to ensure adequate protection while preserving the capacity for humanitarian action. In particular, its intervention influenced negotiations on the very definition of an IO, the proportionality of the obligations imposed on controllers, the management of sensitive data (particularly health or biometric data), and cooperation between supervisory authorities and non-State entities.

Adherence to, or alignment with, Convention 108+ enables IOs to benefit from several strategic advantages, such as enhanced legitimacy and transparency: by adopting an internationally recognised instrument, IOs can demonstrate their commitment to fundamental rights, which is particularly important in contexts of institutional distrust. By working within a common framework, they foster their relations with States, particularly with regard to transborder data transfers.[30]

Through taking part in the Committee's meetings, IOs gain access to a rich normative environment that can help them improve their internal practices, as well as a network of experts that forms the basis for cooperation with national supervisory authorities.

Conclusion

Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is the only legally binding international data

30 Massimo Marelli, "Transferring personal data to international organizations under the GDPR: An analysis of the transfer mechanisms", *International Data Privacy Law*, vol. 14, no. 1 (2024): 19–36, https://doi.org/10.1093/idpl/ipad022.

protection treaty of universal scope to date. This open and universal character is strengthened by the amending Protocol, now Convention 108+, which offers a data protection regime to all States and IOs concerned with ensuring respect for human rights and fundamental freedoms when processing personal data.

By working to extend the number of jurisdictions with data protection legislation based on a common protection framework, while taking into account the diversity and specific features of various legal systems, Convention 108+ promotes the free circulation of personal data between the Parties, while ensuring greater effectiveness of the right to data protection, particularly through the establishment of a mechanism for verifying the conformity of the Parties' domestic law with the requirements of the Convention. Convention 108+ is expected to play a fundamental and central role in the development of a universal right to data protection. IOs, alongside the Council of Europe, can contribute to achieving this essential objective for the future of human rights and fundamental freedoms.

11

DATA PROTECTION, HUMANITARIAN ACTION, AND GLOBAL REGULATORY COOPERATION

The Role of the Global Privacy Assembly

Catherine Lennman and Florence Dubosc

Introduction

This chapter will first set out the Global Privacy Assembly's (hereafter the Assembly or GPA) evolution from an informal gathering of data protection authorities (DPAs) into a leading international forum advancing regulatory convergence, with key milestones, resolutions, and strategic priorities. We will then assess the GPA's contributions and limitations as well as its practical impact. Finally, we focus on how the GPA has operationalised its work in the humanitarian sector through the Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management (WG AID) as well as outlining future directions for enhancing global regulatory cooperation.

A Global Convergence Forum

For over four decades, the GPA – formerly known as the International Conference of Data Protection and Privacy Commissioners (ICDPPC) – has served as the leading global forum for data protection and privacy regulators. Initially established in 1979 in Bonn as a loosely organised annual gathering of European data protection authorities, the Assembly has progressively evolved into a structured, globally representative body. Its transformation over time mirrors broader shifts in data governance, particularly the increasing need for regulatory cooperation across borders in response to globalisation, digitalisation, and the expansion of data-driven services.

In the early years, the Assembly primarily facilitated information-sharing and the cultivation of informal networks among national regulators. However,

DOI: 10.4324/9781003650164-16

as data protection emerged as a legal and political priority worldwide, the Assembly undertook formalisation measures, such as the adoption of resolutions (starting in 1989), the creation of an accreditation mechanism, and the establishment of a permanent Secretariat. By 2010, the creation of an Executive Committee had added governance and strategic oversight functions to the Assembly's remit.

Today, the GPA encompasses over 130 accredited member authorities and more than 30 observers, including key international organisations (IOs) and other public entities. These members span jurisdictions of various types and sizes, stages of regulatory maturity, and legal traditions – from long-established authorities such as the British Information Commissioner's Office (ICO) and the French *Commission nationale de l'informatique et des libertés* (CNIL), to more recently constituted regulators such as the Kenyan Office of the Data Protection Commissioner (ODPC). This inclusive composition fosters peer exchange between advanced and emerging authorities, allowing mutual learning and technical collaboration that supports consistent data protection standards worldwide.

The observer community includes influential actors such as the International Committee of the Red Cross (ICRC), the International Organization for Migration (IOM), the World Food Programme (WFP), and the United Nations (UN) High Commissioner for Refugees (UNHCR). Their participation enables cross-sectoral reflection, particularly on issues where humanitarian mandates intersect with regulatory expectations.

The GPA plays a foundational role in shaping international regulatory convergence by enabling national and regional authorities to coordinate their approaches, develop shared normative frameworks, and exchange operational expertise to foster a more coherent, principled global privacy landscape. This is how the Assembly's annual conferences, hosted by rotating member authorities across six continents, have matured into globally significant policy events. They function not only as discussion platforms but also as operational incubators where resolutions are drafted, normative standards are proposed, and multilateral strategies are devised. These gatherings often serve as the launching point for collaborative initiatives, such as joint capacity-building programmes and thematic working groups. The conferences also provide space for addressing emerging issues such as artificial intelligence (AI), cross-border enforcement, or the data protection implications of humanitarian crises. As a result, the GPA has become a central node in the ecosystem of global data protection governance. In this way, the GPA not only cultivates a global regulatory ethos, but also addresses practical gaps in enforcement, capacity, and interoperability. Its influence derives less from coercive authority and more from its ability to convene, disseminate, and legitimise policy approaches that resonate across legal cultures and institutional contexts.

The GPA's mission is to advance privacy and data protection as fundamental rights – as reaffirmed in its 2019 Resolution on Privacy as a Fundamental Human Right[1] – while promoting regulatory convergence and supporting effective implementation across diverse legal systems. The Assembly aims to serve as a fulcrum for global privacy governance, facilitating a harmonised approach to data protection that recognises both regional legal traditions and the increasing ubiquity of transnational data flows.

This convergence effort is achieved through normative outputs such as resolutions, model frameworks, and strategic plans, as well as through its working groups and collaborative fora. The Assembly's approach to implementation is characterised by a soft-law methodology, privileging mutual learning, consensus-building, and peer cooperation over formal treaty-making. Its collaborative model is structured to empower both mature and emerging DPAs to operate autonomously while aligning with global best practices. Crucially, the GPA provides a neutral platform where regulators, observers – including humanitarian actors and academic experts – and other stakeholders can co-develop guidance, respond to emergent risks, and shape shared priorities through evidence-based deliberation.

The GPA's Contributions and Limitations

In this section, we examine the evolving role of the GPA in advancing regulatory convergence in data protection. We also address the Assembly's practical influence, the coherence of enforcement efforts, and the reach of its capacity-building initiatives.

From Regional Meetings to Global Impact

The GPA first convened in Bonn, Germany, in 1979, followed by Ottawa, Canada, the following year. For the first two decades, its meetings were largely hosted in Europe, with occasional sessions in Canada and Australia. The 21st Conference in Hong Kong (1999) marked a turning point, signalling a shift towards a truly international scope. Since then, the GPA has met on six continents and has embraced a transparent, rotating host model to ensure global representation.

Annual conferences combine plenary sessions, thematic workshops, and the adoption of resolutions and declarations. Notable milestones include the

1 GPA, *Resolution on Privacy as a Fundamental Human Right*. October 2019, https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf.

Madrid Resolution[2] (2009), a landmark text that established the International Standards on the Protection of Personal Data and Privacy. This resolution laid out key principles such as lawfulness, purpose limitation, data quality, accountability, and transparency, aiming to serve as a global baseline and foster harmonisation across jurisdictions. The GPA also adopted the Bermuda Declaration[3] (2023), which underscored the need to develop globally interoperable privacy frameworks and highlighted the importance of multistakeholder engagement in shaping these norms. It particularly encouraged emerging economies and smaller jurisdictions to play a more active role in global standard-setting. The Montreux Declaration[4] (2005), similarly, reaffirmed privacy as a universal human right and emphasised the imperative of fostering meaningful international regulatory cooperation to combat growing cross-border data challenges.

Together, these declarations not only reflect the GPA's evolving normative authority but also provide the institutional scaffolding for subsequent initiatives, such as its working groups on AI, ethics, enforcement cooperation, and humanitarian data protection. They serve as foundational texts for the GPA's role in driving convergence, supporting dialogue, and translating principles into action in an increasingly complex global data ecosystem.

Strategic Vision: The GPA's 2023–2025 Objectives

Building on its evolving institutional role and historical milestones, the GPA has charted a forward-looking strategic plan that addresses contemporary challenges in data protection. The transition from historical development to strategic focus reflects the Assembly's shift from norm-setting to practical, measurable implementation.

In its current Strategic Plan[5] (2023–2025), the GPA outlines three overarching priorities:

2 GPA, *The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy*, 31st International Conference, Madrid, 2009, https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf.

3 GPA, *Resolution on Achieving Global Standards for Data Protection and Privacy*, 45th International Conference, Bermuda, 2023, https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf.

4 GPA, *The Montreux Declaration*, 27th International Conference, Montreux, 2005, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf.

5 GPA, *GPA Strategic Plan 2023–2025*, https://globalprivacyassembly.org/wp-content/uploads/2024/02/GPA-Strategic-Plan-final-version-update-oct10-1.pdf.

1. High Level of Data Protection in Global Frameworks: the GPA has made it a priority to influence and support the development of international standards and frameworks, ensuring equitable protection of vulnerable groups including children, women, migrants, and indigenous peoples. One of the notable advancements on this topic has been the adoption and promotion of the Resolution on Achieving Global Data Protection Standards.[6] This Resolution aims to positively influence data protection laws, policies, and practices by establishing key principles and rights essential for high data protection standards. Recognising that high global data protection standards are vital to providing increased protections for people and certainty for organisations, this Resolution seeks to foster a common understanding of standards and approaches to data protection among the data protection and privacy authorities of the world. By outlining essential principles and rights, the GPA aims to create a framework that member authorities can adopt, ensuring robust data protection practices are universally implemented. Building on the GPA's 2009 Madrid Resolution,[7] the 2023 Resolution updates and emphasises high-level principles crucial for data protection in the digital age.

In 2024, a Resolution on Data Free Flow with Trust and an effective regulation of global data flows[8] were adopted in order to advocate for and promote high standards for data protection and privacy.

This objective has also been operationalised through the GPA's active engagement with multilateral processes, such as contributions to the Organisation for Economic Co-operation and Development's (OECD) data governance work and collaboration with the UN Special Rapporteur on the Right to Privacy;

2. Strategic Alliances and Impact: to foster partnerships with authorities, networks, and organisations, enhancing the GPA's impact on global privacy and data protection policy. Implementation of this objective has included the formalisation of observer status for IOs and public entities, joint policy papers on topics such as international data transfers and AI governance, and shared statements with regional privacy networks such as the Asia Pacific Privacy Authorities (APPA) and the Network of African

6 GPA, *Resolution on Achieving Global Data Protection Standards*, October 2023, 3.-Resolution-Achieving-global-DP-standards.pdf.

7 GPA, *The Madrid Resolution*.

8 GPA, *Resolution on Data Free Flow with Trust and an effective regulation of global data flows*, November 2024, https://globalprivacyassembly.org/wp-content/uploads/2024/11/Resolution-Data-Free-Flow-with-Trust-and-an-effective-regulation-of-global-data-flows.pdf.

Data Protection Authorities (NADPA). The GPA has also supported strategic dialogues between regulators and industry stakeholders. The GPA has strengthened its engagement with external stakeholders, such as other sectoral regulators, and the scientific/academic sector, e.g. the creation of a reference panel[9] which is a diverse contact group of external stakeholders that support the GPA and its members by providing expert knowledge and practical expertise on data protection and privacy, as well as on data protection-related issues and developments in information technology, thereby equipping the GPA with the ability to identify cross-disciplinary policy solutions to privacy and data protection issues;

3. Capacity-Building for Data Protection Authorities: to promote peer learning, the exchange of best practices, and the creation of tools and mechanisms that facilitate practical enforcement and policy implementation. This has led to the establishment of dedicated capacity-building workshops, twinning programmes between mature and emerging DPAs, and the development of toolkits such as maturity models for regulatory self-assessment. The work of the International Enforcement Cooperation Working Group (IEWG) is an excellent example as it is an active group considering live issues and concerns related to enforcement, with a focus on sharing experience, tactics, and approaches to tackling specific aspects, including common experiences in investigating multinational companies.

In its next Strategic Plan (2025–2027), which should be adopted at the 47th GPA in Seoul in September 2025, members will continue working on these three objectives, continuing to connect the efforts of DPAs, focusing on supporting and influencing the development of international standards and frameworks that promote the human right of personal data protection, strengthening data protection and privacy enforcement authorities, and generating ethical standards that guide the development of the digital ecosystem.

Global Engagement: Human Rights, Humanitarian Action, and Practical Impact

The GPA's engagement with humanitarian data protection has deepened notably over the past decade. Its 2015[10] and 2020[11] resolutions established a foundational mandate for collaboration between DPAs and humanitarian

9 GPA Reference Panel, https://globalprivacyassembly.org/gpareferencepanel/.

10 37th International Conference of Data Protection and Privacy Commissioners, 9 April 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

11 GPA, *Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management*, October 2020, https://

organisations. These resolutions encouraged risk-aware, rights-based approaches to data processing in emergencies.

The GPA's alignment with international human rights initiatives is central to its evolving identity. In April 2015, the Assembly welcomed the appointment of the first UN Special Rapporteur on the Right to Privacy,[12] a move that reinforced the Assembly's commitment to embedding privacy within global human rights governance.

Similarly, in 2017, the GPA acknowledged the significance of the Handbook on Data Protection in Humanitarian Action[13] (Handbook), co-produced by the Brussels Privacy Hub and the ICRC, as a milestone in humanitarian privacy practice. Various regional networks of DPAs, such as the *Association Francophone des autorités de protection des données personnelles* (AFAPDP) and the Ibero-American Data Protection Network (RIPD), have also promoted this important tool through their members and conferences, e.g. conferences in Burkina Faso and Tunisia.

The Handbook's development has been closely tied to the GPA's broader normative ecosystem. It has supported alignment between DPAs and humanitarian actors, offering a shared vocabulary and practical toolkit that facilitate regulatory compliance even in fragile and conflict-affected contexts. It was conceived as a continuation of the dialogue initiated by the ICDPPC's 2015 Resolution on Privacy and International Humanitarian Action.[14] It does not seek to replace applicable legal obligations or internal organisational policies. Rather, it aims to raise awareness and assist humanitarian organisations in complying with data protection standards, especially in the use of new technologies, for example in the creation of a certification and training programme for data protection officers which will be discussed later. The Handbook provides concrete guidance for interpreting data protection principles in humanitarian contexts, including when deploying digital identity systems, mobile-based cash transfers, or biometric registration. It has since become one of the most widely cited and operationalised tools in the humanitarian sector, offering a concrete interpretation of data protection principles tailored to the ethical and logistical complexities of crisis response.

---

globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-International-Aid-EN.pdf.

12 ICDPPC, *Global Data Protection Commissioners Welcome UN Privacy Announcement*, 9 April 2015, https://globalprivacyassembly.org/wp-content/uploads/2016/01/Global-Data-Protection-Commissioners-welcome-UN-privacy-announcement.pdf.

13 Christopher Kuner, Massimo Marelli, and Vagelis Papakonstantinou, eds., ICRC Handbook on Data Protection in Humanitarian Action (2017 edition).

14 ICDPPC, Resolution on Privacy and International Humanitarian Action, 27 October 2015, https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

Concrete instances of the GPA's influence can also be seen in the field. For example, the Kenyan Office of the Data Protection Commissioner collaborated with humanitarian actors on training programmes for data protection officers working in displacement and crisis contexts. These efforts reflect a growing emphasis on national-regional cooperation catalysed by the GPA's normative output.

Furthermore, the GPA has promoted field-based dialogue involving domestic DPAs and IOs in crisis zones such as Senegal and Kenya, often via working group intermediaries. These engagements underscore the GPA's pragmatic role in enabling not only policy formulation but also cross-border operational interoperability in complex, data-intensive environments.[15]

In 2024, the publication of the third edition of the Handbook further solidified its role as a living document responsive to emerging technologies, such as AI-powered needs assessments and blockchain-based cash assistance. Given the Handbook's strategic significance and the contributions of the WG AID, the Executive Committee of the GPA decided to formally endorse the third edition. Beyond formal recognition, the Executive Committee has actively supported the Handbook's dissemination, promoting it through working group sessions, official communications, and conference programming. This action underscores the GPA's strong commitment to practical tools that support both regulatory convergence and effective humanitarian data governance.

Institutional Developments and Normative Contributions to Humanitarian Data Protection

There remains, however, an ongoing challenge in aligning the enforcement and accountability mechanisms of IOs with those of domestic DPAs, some of which are newly created or still being set up and lack experience in this area. Experts from certain DPAs and members of the WG AID are involved in helping to set up authorities, for example in Madagascar. While the GPA has offered a shared platform for dialogue, enforcement cooperation remains fragmented due to jurisdictional limitations, operational silos, and differing legal mandates.

Looking ahead, the GPA could bolster enforcement alignment by expanding its current working groups to include specific clusters on cross-jurisdictional enforcement, emergency response, and private sector accountability in humanitarian operations. The GPA's engagement with humanitarian data protection has deepened notably over the past decade, and this evolution is closely reflected in the subsequent case studies that illustrate how core

15 See Chapter 19, "Teaching Data Protection as Trust Building".

principles enshrined in GPA resolutions have translated into operational practice. These examples bridge the gap between normative development and field implementation, making explicit the GPA's role in shaping responsible data governance in humanitarian action, reflecting a growing recognition that personal data plays a central role in crisis response and recovery.

The 2015 Resolution on Privacy and International Humanitarian Action[16] was a formative moment in the GPA's history, acknowledging the pressing need to adapt privacy safeguards to operational realities on the ground. This Resolution underscored the importance of responsible data collection, processing, and sharing in humanitarian settings and recognised that data misuse can expose already vulnerable populations to additional harms such as surveillance, discrimination, or retribution. Building on this foundation, the 2020 Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management[17] reaffirmed the Assembly's commitment and broadened the focus. It explicitly called for the integration of data protection considerations into all phases of humanitarian response, from preparedness and coordination to long-term recovery.

The establishment of a dedicated working group, the aforementioned WG AID, has been instrumental in translating these commitments into action. Its 2024 Annual Report[18] highlights progress in facilitating structured dialogues between IOs and domestic regulators, fostering mutual understanding, and developing shared tools. It documents evolving good practices in areas such as biometric registration, digital identity, and data ethics in crisis response.

Despite its normative reach, the GPA faces ongoing challenges in translating resolutions and declarations into consistent practice. As non-binding instruments, GPA outputs depend on voluntary adoption and political will. This has led to uneven implementation across member jurisdictions. While this challenge is not unique to the GPA – it is emblematic of the broader limitations of soft law in data governance – it raises important questions about follow-up, accountability, and the mechanisms required to move from consensus to concrete impact. Given the current budgetary cuts within IOs, we fear it could lead to the deprioritisation of the topics worked on by the GPA, making it more challenging to implement consistent practice in the sector.

16 ICDPPC, Resolution on Privacy and International Humanitarian Action.

17 GPA, *Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management.*

18 GPA, *Humanitarian Aid and Crisis Management: Annual Report.* 2024, https://globalprivacyassembly.org/wp-content/uploads/2024/11/4.-Humanitarian-Aid-and-Crisis-Management-2024-Annual-Report_EN-final.pdf.

Among the Assembly's early contributions, the 2003 Resolution on Data Protection and International Organisations[19] was particularly significant. It urged IOs to adopt internal data protection regimes aligned with international standards, while encouraging national regulators to engage constructively with IOs. This pioneering Resolution addressed legal pluralism and sought practical avenues for cooperation.

Recent academic work further explores these intersections. In a 2023 article in Computer Law and Security Review,[20] Marelli analyses how IOs navigate between domestic legal regimes and their own internal standards. This analysis is further elaborated in an analysis of the Headquarters' Agreement between the ICRC and Luxembourg for the establishment of the ICRC Delegation for Cyberspace.[21] In a related 2023 publication in International Data Privacy Law,[22] Marelli assesses GDPR-compliant mechanisms for data transfers to IOs. Together, these works highlight the legal intricacies and governance dilemmas that the GPA seeks to manage through structured dialogue and cooperative resolution-building, especially when developing normative standards; this is done in particular through GPA working groups.

Finally, these developments must be understood in the context of broader international standards, including the 1990 UN Guidelines on Regulating Computerised Personal Data Files,[23] which continue to shape expectations around oversight, accountability, and the protection of individual rights in international data practices.

The momentum generated by these frameworks culminated in the GPA's 2020 Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management. This landmark Resolution not only reaffirmed the Assembly's recognition of

19 GPA, *Resolution on Data Protection and International Organisations*, 25th International Conference, Sydney, 12 September 2003. https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-International-Organisations.pdf.

20 Massimo Marelli, "The Law and Practice of International Organisations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads Between the International and Domestic Legal Orders," *Computer Law and Security Review*, 2023, https://www.sciencedirect.com/science/article/pii/S0267364923000596.

21 Andrea Raab and Massimo Marelli, "Inviolability in the digital era: The ICRC's Agreement on Privileges and Immunities with Luxembourg," *International Review of the Red Cross* (2025): 1–28, https://doi.org/10.1017/S1816383125000190.

22 Massimo Marelli, "Transferring Personal Data to International Organizations under the GDPR: An Analysis of the Transfer Mechanisms," *International Data Privacy Law* 14, no. 1 (2023): 19–36. https://doi.org/10.1093/idpl/ipad022.

23 UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 1990, https://www.refworld.org/policy/legalguidance/unga/1990/en/13761.

the unique data protection challenges inherent to humanitarian settings, but also mandated the formal creation of the WG AID.

The Establishment of a Dedicated Working Group

Tasked with translating policy into practice, the WG AID brings together State regulators and regulators of IOs engaged in humanitarian action to collaboratively develop guidance, coordinate training, and assess evolving risks in fragile contexts. It has since become one of the GPA's most active working groups, delivering annual reports and playing a central role in fostering international regulatory dialogue.

The leadership of the WG AID has notably benefited from the engagement of smaller, yet strategically placed, data protection authorities, including those of Switzerland (FDPIC), Monaco (APDP), Argentina (AAIP), Benin (CNIL), Ivory Coast (ARTCI), Gabon (CNPDCP), Kenya (ODPC), Niger (HAPDP), and Senegal (CDP).

The establishment and activities of the WG AID thus represent a pivotal institutional innovation, marking a sustained commitment to practical collaboration between regulators.

Understanding the Notions of International Development Aid, International Humanitarian Aid, and Crisis Management

From an operational standpoint, the first action of the WG AID was to identify the relevant actors, in terms of development aid, humanitarian aid, and crisis management by drawing up a map and sending out a questionnaire[24] to the key players in this field.

These tasks revealed the complexity for an outsider to develop a concise overview of development assistance, humanitarian aid, and crisis management due to the many entities involved and the increasing complexity of humanitarian crises.

The competencies of development agencies and humanitarian organisations may in fact come into collision and the WG AID felt it was necessary, in preparing its action plan, to separate, on one hand, the main donors who do not intervene in the implementation of programmes and, on the other, the IOs and operators who ensure such implementation.

Moreover, any data collected, no matter how trivial, can be sensitive, since in some regions a simple name can reveal a person's ethnic origin or religious

24 GPA, *Annual Report 2021 of the WG AID, Annex 4 "Questionnaire on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management,"* 1.3k-version-4.0-Humanitarian-Aid-Working-Group-EN-adopted.pdf.

affiliation. The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally.

In practice, it has emerged from the research carried out by the WG AID that the implementation of data protection guidelines and policies is often inconsistent across humanitarian response contexts, despite the international standards available and the efforts made by many humanitarian actors.

A systemic and global approach is therefore necessary and it is with this in mind that the WG AID intends to develop its actions.

Identifying Key Topics and Challenges

Despite the low response rate to its questionnaire, the WG AID managed to identify a wide range of topics due in large part to the increasing importance of digital technology in the projects implemented as part of international development aid, humanitarian aid, and crisis management, which can potentially rely on the use of personal data.

Drones can now deliver medicines to remote areas that were previously inaccessible and biometric devices can enable migrants to establish their legal identity and thus gain access to public assistance. While these technologies today offer unique opportunities that can bring about real, significant change by helping millions of people, they must nevertheless be conceived as strategic, inclusive, and well-designed tools in order to ensure data protection.

However, this development of newer technologies and humanitarian data management standards and practices generally evolves more rapidly than the institutional frameworks that regulate their use, resulting in uncertainty and a lack of coordination.

De facto, from a data protection perspective, these technical innovations raise significant data protection and privacy issues[25] that may result in harm to people's dignity, physical harm or damage to personal safety, discrimination, exclusion or lack of assistance, or social stigmatisation, reputational damage for data subjects, such as limited control over their personal data, unauthorised collection, use, retention or disclosure, automated decision-making through profiling, and identity fraud through the misuse of digital IDs. Yet, these populations have experienced trauma or have special needs, and the data

25 Ana Beduschi, "Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks," *International Review of the Red Cross,* 104, no. 919 (2022): 1149–1169, https://doi.org/10.1017/S1816383122000261.

Keren Weitzberg et al., "Between surveillance and recognition: Rethinking digital identity in aid," *Big Data and Society*, 1 April 2021, https://journals.sagepub.com/doi/full/10.1177/20539517211006744#tab-contributors.

collected often includes highly sensitive personal data, including details of the abuse they suffered, requiring strict policies and procedures to be in place.

Another concern that has been raised by the respondents to the WG AID questionnaire is the fear that sensitive data collected by humanitarian actors in the course of their action may end up being acquired by private companies that were not part of the original humanitarian response through, for instance, the use of technologies such as biometric registration processes, cloud-based platforms, or AI and advanced analytics. For example, many worry about a possible risk of commercialisation of data by these companies or further processing/harnessing of the data. This is creating an unequal power structure that affects beneficiaries.

In addition, the WG AID noted from the answers to the questionnaire a lack of common definitions of key data protection concepts, which can lead to misunderstandings of the terminology used, as well as a lack of risk mitigation measures and accountability mechanisms. Too often, such mechanisms are left outside the margins in practice and sometimes in policies too, despite it being important in implementing data protection standards. This raises questions such as: what is the responsibility of humanitarian organisations as regards data protection? And what accountability mechanisms are available for beneficiaries?

When it comes to requests for data sharing, the expectation of partners also seems to vary according to factors such as the complex regulatory frameworks for data (e.g. host or donor government law, particularly in the context of privileges and immunities for non-governmental organisations), the types of agreement (e.g. grants or contracts), and funding allocations (e.g. project-specific vs non-earmarked funding). Besides, the level of detail in the information requested may in practice differ from one situation to another.

Lastly, there are significant gaps in existing guidelines and standards, particularly in relation to assessing the sensitivity of the data collected and the particular challenges of protecting personal data in development assistance, humanitarian aid, and crisis management.

A Heterogeneous Range of Players to Consider

The diversity of players involved in humanitarian action, whether they be UN entities, other IOs, non-governmental organisations, or other players involved in implementing and coordinating humanitarian action, must also be taken into account by the WG AID in the elaboration of its working plan.

If most IOs have a good degree of maturity and awareness in terms of personal data protection – as evidenced in particular by the data protection

policies already in place, e.g. the ICRC's Data Protection framework,[26] UNHCR's Data Protection Policy,[27] or which are currently being revised or drafted, e.g. IOM[28] – the situation is often different with non-profit organisations. In fact, some of them may have limited resources or may quickly find themselves overwhelmed by the complexity of the issues they face.

Those headquartered in the European Union are now for the most part well aware of the General Data Protection Regulation (GDPR), but the situation becomes more complicated when they have to carry out missions, for instance, in Africa, Asia, or South America, where the lack of a unified approach between countries increases the risks for both stakeholders and data subjects.

Indeed, in some countries, comprehensive legislation on the protection of personal data is in place, with appropriate authorities (Colombia, Senegal, and Kenya, for example), while in others, there is no legislation or protection framework (Afghanistan, Myanmar, or Venezuela).

Finally, there has also been a high demand for support in the field from States, in particular development agencies, especially when implementing assessment tools and guidance meant to advise their staff, consultants, and partners working on financed projects that use digital tools or solutions.

The Importance of Strengthening Cooperation with the Main Actors

As members or observers of the GPA, IOs have a large role to play within the working group.

Since its creation, the WG AID has thus developed close collaboration with the ICRC, which has included the participation of some of its members in the review and translation of the Handbook on Data Protection in Humanitarian Action.

As noted previously, the WG AID is now actively promoting this manual via the different regional networks of DPAs, such as the AFAPDP.

A significant outgrowth of these collaborative efforts is the development of a specialised certification and training programme for Data Protection Officers in Humanitarian Action, jointly initiated by the Data Protection Office of the ICRC and the European Centre on Privacy and Cybersecurity

26 ICRC Rules on Personal Data Protection, 2020, https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

27 UNHCR, Policy on the Protection of Personal Data of Persons, 2015, https://data.unhcr.org/en/documents/details/44570.

28 IOM, Data Protection Manual, 2010, https://publications.iom.int/system/files/pdf/iom-dataprotection_web.pdf.

at the University of Maastricht, with the active involvement of the GPA's WG AID.[29]

The certification course builds on the lessons embedded in the Handbook and aims to equip data protection officers with the legal, technical, and operational skills necessary to uphold data protection principles in emergency contexts. Its launch and expansion represent a practical and innovative manifestation of the GPA's commitment to knowledge diffusion, capacity-building, and real-world impact in fragile and conflict-affected environments.

Joint actions have also been initiated with IOM, UNHCR, and WFP, among others, resulting in panels at various international fora and the forthcoming hosting of webinars.

The aim in the future is to cooperate more closely, especially through guidelines on specific issues, such as how best to deal with data breaches or requests to share data, and without further complicating humanitarian action, but rather facilitating it. In this respect, it is worth noting that, according to the answers to the questionnaire, organisations with privileges and immunities have also recently come under significant pressure to share their data.

Moreover, the WG AID understands that while many IOs are keen to cooperate with DPAs on standards and guidance, they still need to do their own compliance and enforcement.

While they do not in principle have to apply domestic laws, they are often faced with practical dilemmas, for instance, when dealing with their service providers. Often, while they want these service providers to comply with national data protection legislation, they also consider that the latter must respect their privileges and immunities and at times limit the reach of domestic law in this context.

Even if these collaborations with IOs active in humanitarian emergencies are still in their infancy, they have already proven to be effective in bringing data protection to places where domestic laws are not applied or enforced due to fragility or conflicts (through, for instance, the organisation of conferences). Annual sessions of the Data Protection Officer in Human Action Certification are now also being organised in Nairobi, thanks in part to the impetus of the Kenyan Office of the Data Protection Commissioner.

Collaboration with non-governmental organisations, however, takes a different form. As the latter are not members or observers of the GPA, the WG AID intends to be considered more as a pool of expertise and a privileged interlocutor to meet their specific needs.

The aim is to support them in their day-to-day activities in the field, both upstream by helping them put in place procedures to protect personal data (by applying, for instance, the data minimisation and purpose limitation

29 Chapter 19, "Teaching Data Protection as Trust Building".

principles) and downstream by advising them on good practice in the event of security breaches, for example.

A number of challenges have already been identified, including often a lack of capacity in terms of technical skills, time constraints, and technical infrastructure. Information documents, case studies, and training courses are being developed to address these issues.

Finally, a sub-working group has been set up with the data protection officers of the Association of European Development Finance Institutions (EDFI) in order to strengthen the sharing of resources and learning. One of the goals of this group is to adopt a human rights-based approach by raising awareness of how to strengthen human rights within a project cycle, and by supporting efforts to ensure that the digital projects, digital solutions, and tools being developed do not negatively impact human rights.

Exploring Synergies with Other Working Groups

As previously mentioned, the WG AID is just one of many other working groups within the GPA and its action could be strengthened through collaboration with some of them.

For example, projects are currently being developed with the GPA's Data Protection and Other Rights and Freedoms Working Group (DPORF) created in 2019. Personal data protection must be designed to respect, protect, and promote human rights. This includes fundamental freedoms and the exercise of others' human rights, such as freedom of movement or opinion, asylum, non-refoulement, and procedural guarantees.

The goal is to develop methods and approaches that could be used complementarily in order to obtain optimal protection outcomes.

In order to prevent and or mitigate the risks posed by AI systems, joint actions could also be undertaken in the near future with the GPA's Working Group on Ethics and Data Protection in Artificial Intelligence[30] to develop best practices. AI is now increasingly used in the humanitarian field, for instance for data analysis or to help develop sustainable solutions in climate action, and the goal of DPAs is not to curtail the positive impact it can have on humanitarian efforts but rather to learn to appreciate its full scope in order to prevent any risks to personal data.

The WG AID strongly believes that all these actions should contribute to building a global privacy community committed to high standards of protection of individuals' privacy, particularly for those who are beneficiaries of

30 GPA, Working Group on Ethics and Data Protection in Artificial Intelligence, 2024, https://globalprivacyassembly.org/wp-content/uploads/2024/11/8.-Ethics_and_Data_Protection_in_AI_Working_Group_Annual_Report.pdf.

international development or humanitarian aid programmes and who are particularly vulnerable.

Conclusion

The evolution of the GPA from an informal DPA gathering into a leading international forum advancing regulatory convergence has helped achieve increasingly effective regulator-humanitarian collaboration.

In essence, the GPA demonstrates how sustained and inclusive dialogue grounded in soft-law tools like resolutions and peer learning can bridge legal traditions and drive coherent global data protection and privacy. It does so by convening State regulators (i.e. DPAs), IOs active in the humanitarian sector, and experts, particularly through working groups and by translating principles into deliverables.

Since its creation, the WG AID has therefore worked to develop close ties with actors in the field and identify ever-changing challenges in data protection in order to become a true pool of expertise and a key point of contact for responding to the specific needs of the humanitarian sector. It is in this context that the GPA, through its WG AID, is currently promoting the Handbook, which is a good example of how to turn consensus into capacity, interoperability, and real-world impact.

All this ongoing work contributes to building a global privacy community committed to high standards of protection of individuals' privacy, particularly for those who are beneficiaries of international development or humanitarian aid programmes and who are particularly vulnerable.

PART 3.2

Data Protection Law in Humanitarian Practice

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

12

DATA PROTECTION IN THE FRAMEWORK OF RESTORING FAMILY LINKS HUMANITARIAN ACTIVITIES

Code of Conduct and Resolutions

Emily Knox[1]

Introduction

Restoring Family Links (RFL)[2] is one of the original services of the International Red Cross and Red Crescent Movement (the "Movement"), first carried out by founder Henry Dunant following the Battle of Solferino in 1859.[3] In the years after, National Societies were created around the world, which to this day continue to look for missing family members in contexts of conflict, disaster, and migration.

Whilst the International Review of the Red Cross (IRRC) has published a body of literature on RFL[4] and there have been a few academic papers on

1 The opinions and views expressed in this chapter are the author's own and do not necessarily reflect those of the British Red Cross.

2 "Restoring family links is a term that covers a wide range of activities, all designed to alleviate the pain of separation among loved ones. These include: organizing the exchange of family news, tracing individuals, registering and keeping track of individuals to prevent their disappearance and to enable families to be informed about their fate, and reuniting families." Source: ICRC, Restoring Family Links: Presenting the Strategy for a Worldwide Network (2009). This leaflet summarized the work being done by the Family Links Network of the International Red Cross and Red Crescent Movement to meet the needs of those separated. It also presented the actions defined by the 2008-2018 10-year RFL Strategy to improve services, cooperation and support for the restoration of family links. ICRC, Geneva, 2009

3 Henry Dunant fulfilled the wish of a 20-year-old dying soldier, Claudius Mazuet, by passing on a message to his parents letting them know their son's fate: until this, Mazuet had been categorised as missing. "A Memory of Solferino," ICRC, accessed 22 April 2025, 66, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0361.pdf.

4 Anjli Parrin, "'How did they die?': Bridging humanitarian and criminal-justice objectives in forensic science to advance the rights of families of the missing under international

DOI: 10.4324/9781003650164-18

RFL,[5] there has been no specific focus on the RFL Code of Conduct on Data Protection ("the Code") from 2015.[6] A decade after its inception, this chapter looks at the creation and application of the Code, providing an assessment of the challenges and benefits of operationalising a global set of standards.

Restoring Family Links is described as "a range of activities aimed at preventing family separation and disappearance of persons, restoring and maintaining contact between family members, reuniting families, and contributing to clarifying the fate of persons reported missing".[7] It is at the core of the humanitarian imperative to alleviate suffering: on an interpersonal level, providing a life-changing service to those forced apart, with people affected by the ambiguity of not knowing where loved ones are, or being physically separated for years on end, suffering psychologically and physically.[8] As one father described:

---

humanitarian law," IRRC No. 923, June 2023, https://international-review.icrc.org/articles/how-did-they-die-bridging-humanitarian-and-criminal-justice-objectives-923.

Alexandra Ortiz, and Ximena Londoño "Q&A: The ICRC's engagement on the missing and their families," Editorial: The missing, Vincent Bernard, Implementing international law: An avenue for preventing disappearances, resolving cases of missing persons and addressing the needs of their families, IRRC No. 905, August 2017, https://international-review.icrc.org/articles/implementing-international-law-avenue-preventing-disappearances-resolving-cases-missing.

Olivier Dubois, Katharine Marshall, and Siobhan Sparkes McNamara, "New technologies and new policies: the ICRC's evolving approach to working with separated families," IRRC No. 888, December 2012, https://international-review.icrc.org/articles/new-technologies-and-new-policies-icrcs-evolving-approach-working-separated-families.

5 Secen Sefa, and Mostafa Shalaby, "Living with Absence, Missing Migrants and the Red Cross and Red Crescent's Restoring Family Links Program," *Muslim World Journal of Human Rights* 19, no. 1 (2022): 129–141; Kristin Bergtora Sandvik, "The centralization of vulnerability in humanitarian cyberspace: the ICRC hack revisited," *Humanitarian extractivism* (Manchester University Press, 2023): 38–56.

6 Current RFL Code of Conduct on Data Protection, Version 2.0, ICRC (2024) accessed 24 May 2025, https://www.icrc.org/en/document/rfl-code-conduct. Original Version 1.0 published in 2015, https://rcrcconference.org/app/uploads/2019/07/rfl-code-of-conduct.pdf.

7 Based on internal guidance of the Movement: Introduction to RFL Guidelines https://icrc.sharepoint.com/sites/flextranet/SitePages/RFL-Guidelines.aspx (not publicly available) accessed on the Family Links Extranet (Family Links Network's internal Intranet), 28 February 2025.

8 Humanitarian Consequences of Family Separation & People Going Missing, British Red Cross, International Committee of the Red Cross (ICRC), Red Cross EU Office, Swedish Red Cross, Swiss Red Cross, 2019 chapters 1 and 2, https://redcross.eu/uploads/files/Positions/Migration/Family%20Separation/rapport-2019-humanitarian-consequences-of-family-separation-and-people-going-missing.pdf.

> When I finally saw them, it was like a very big weight on my head was lifted. The British Red Cross really did give me a rebirth because I was like a dead man.[9]

The Movement's RFL work is vast and may include activities such as the tracing of missing people, provision of connectivity such as mobile phones, chargers or Wi-Fi, keeping families in contact with their detained loved ones, creating lists of separated children, physically reuniting families, and supporting the dignified treatment of the dead with a view to supporting their identification. RFL activities of National Societies can differ depending on needs and context. For example, for the Ethiopian Red Cross, connectivity, such as the provision of mobile phones to enable separated family members to call each other, is a large part of the work. Whereas for the British Red Cross, the main services relate to tracing requests from people who have migrated to the United Kingdom (UK) looking for family abroad, or travel assistance for people with refugee status wishing to bring family to the UK using refugee family reunion visas. The resulting challenges in implementing data protection, ethical dilemmas, and potential issues vary from one society to another.

Despite these differences, exchanging personal data internationally is an essential part of reconnecting families, and keeping data safe remains core to the service. Therefore, the changing global landscape of data security, data harm, and data protection regulation is central to the functioning of the Family Links Network (FLN) and the protection of those it serves.

To that end, this chapter will look at the role and practical application of data protection when searching for and reuniting families. It includes the strengths and limits of consent, and focuses on the RFL Code of Conduct on Data Protection. The chapter will emphasise the importance of the Movement's components being permitted to rely on public interest as a legal basis for processing personal data and show how data protection serves as a critical lens that can bring to life the Fundamental Principles of the Movement. The issues will be illustrated through case examples covering areas such as the realities of implementing the Code and checking the applicability of public interest as a legal basis.

Methodologically, the chapter draws on the author's experience leading a tracing and family reunion service and participating in global fora on

9 "Nothing is as painful as being separated from your family" British Red Cross website, accessed 18 February 2025, https://www.redcross.org.uk/stories/migration-and-displacement/refugees-and-asylum-seekers/reuniting-jan-and-his-family?utm_campaign=Every%20Refugee%20Matters&utm_swebource=Salesforce&utm_medium=Email&utm_content=Fundraising_Stewardship_220515_Jans%20story_Copy%201_blog&utm_term=179701_Every%20Refugee%20Matters%20Journey&wu=true.

Restoring Family Links, policy documents and informational material from the Movement, interviews with field practitioners, and academic literature.[10]

Background

The Digital Transformation of RFL

RFL involves activities such as tracing missing people, provision of connectivity such as mobile phones, chargers, or Wi-Fi, sending of Red Cross Messages to and from places of detention, creating lists of separated children, physically reuniting families, and dead body management. These activities are carried out by the FLN,[11] comprising the Central Tracing Agency of the International Committee of the Red Cross (ICRC), RFL units of ICRC delegations, and RFL units of 191 National Societies.[12] The International Federation of Red Cross and Red Crescent Societies (IFRC) also plays an important role in supporting the capacity strengthening of National Societies' RFL units, and integrating RFL in emergencies and migration. Outside the Movement, there are a plethora of non-governmental organisations, family groups, forensic teams, authorities, and intergovernmental organisations, such as the International Commission on Missing Persons (ICMP)[13] and the International Criminal Police Organization (INTERPOL),[14] which also work on the issue of the missing. In the last few years, the ICRC Central Tracing Agency, in partnership with a few National Societies and with the voice of families of the missing at its heart, created the Global Response Missing Persons Centre, which brings together a global community to highlight, research, and offer expertise on preventing and resolving cases of missing persons and addressing the needs of families of the missing.[15]

10 With particular thanks to colleagues for their contributions, including Michael Meyer, Carlos Orjuela, Milgo Ali, Nizam Zanganah, Kristin Bergtora Sandvik, Penny Sims, Pierrick Devidal, Diana Araujo, Davide Cascone, David Owot, Emmanuel Lopia, María Fernanda Carrera Rodríguez, Katherine Wright, Florence Boreil, Lucia Giavitto, Harriet Macey, and Valdet Saiti.

11 Family Links Network, "Who we are," Family Links Network website, accessed 28 February 2025, https://familylinks.icrc.org/who-we-are.

12 "About National Societies," IFRC, accessed 28 February 2025, https://www.ifrc.org/who-we-are/international-red-cross-and-red-crescent-movement/about-national-societies.

13 International Commission on Missing Persons, accessed 27 May 2025, https://icmp.int/.

14 Interpol View Yellow Notices, accessed 27 May 2025, https://www.interpol.int/en/How-we-work/Notices/Yellow-Notices/View-Yellow-Notices.

15 "Missing Persons Global Response," Missing Persons Platform, accessed 26 May 2025, https://missingpersons.icrc.org/.

RFL work is grounded in international humanitarian law, with the Movement legally mandated to conduct restoring family links activities.[16] These are complemented by the Statutes of the Movement; resolutions adopted by statutory bodies of the Movement; and declarations adopted by the regional statutory meetings of the Movement.[17]

Over the last ten years, the FLN has gone through a digital transformation, reflecting changes in society and the sector, and a need to adapt and make use of technology to meet the expectations of those using RFL. The online platform Trace the Face,[18] introduced in 2013 and expanded globally, created a new way of working, and a number of National Societies and ICRC delegations have explored the option of sending DNA profiles digitally overseas in collaboration with States to help families find out the fate of loved ones who may have died en route. Continual review of RFL digital tools has been important as the risks continue to evolve and increase with the changing technological landscape and a rise in data scraping and artificial intelligence.

The creation of a global case management solution, used by a significant portion of National Societies, on the one hand, provides tools for securely transferring data across borders, but, on the other, has led to concerns about humanitarian extractivism with the pooling of vast data sets of people who are in vulnerable situations.[19] In the last few years, the FLN has suffered two significant data breaches.[20] Following the breaches, it has made continuous efforts to

16 Several provisions in the 1949 Geneva Conventions and their 1977 Additional Protocols, including those identified to be customary in nature, refer to the spectrum of Restoring Family Links activities. Restoring Family Links Strategy 2020–2025, Legal Reference, ICRC 65–75.

17 Restoring Family Links: A Guide for National Red Cross and Red Crescent Societies (2008) 14–16, 1.1, shop.icrc.org/restoring-family-links-a-guide-for-national-red-cross-and-red-crescent-societies-en-pdf.html.

18 "Trace the Face," accessed 22 April 2025, https://tracetheface.familylinks.icrc.org/?lang=en. Trace the Face was designed with data protection in mind, the sought person's photograph is never uploaded publicly, and contact with those in the photo is through the local National Red Crescent or Red Cross Society with a human verification process applied. Only the enquirer's photo and the relationship with the person they are looking for are made public, the rest of the personal information about both individuals is kept confidential and metadata is removed from the photograph before publication. It complies with the Protection Standards as set out in Chapter 7 of the Professional Standards for Protection Work. In addition, at the British Red Cross, children (under 18), survivors of trafficking, and people with other vulnerabilities are not considered for Trace the Face. At the time of writing, Trace the Face is offering only private viewings by appointment in some countries whilst a further risk assessment is conducted.

19 Kristin Bergtora Sandvik, "The centralization of vulnerability in humanitarian cyberspace: the ICRC hack revisited," *Humanitarian Extractivism: the Digital Transformation of Aid*, 2023.

20 "ICRC cyber-attack: Sharing our analysis," ICRC, accessed 12 May 2025, https://www.icrc.org/en/document/icrc-cyber-attack-analysis.

strengthen its data protection and cybersecurity.[21] As the evolution and digital transformation of the FLN continues, the normative infrastructure and the way data protection is applied will become even more critical to the Network's legitimacy, preserving trust, accountability, and operational effectiveness.

As we look to the future with digital matching through algorithms[22] and facial recognition,[23] a data protection lens becomes even more important in helping RFL services navigate a digitalised world to counter the new risks that an evolving tech landscape brings while remaining true to the fundamental principles and service user protection.

The Digital Transformation of RFL

Data Protection in the Context of RFL

Data protection has always been important for RFL services. Data is not a by-product of this humanitarian service. It is a critical enabler along with human compassion. The handling of personal data, which may be sensitive, is integral to the provision of humanitarian activities. But it is the humanitarian approach, the empathy, the listening, the protection of people's dignity, and the enabling of hope in the most fraught of times that encapsulates RFL services. People who use the tracing service are by and large those who have fled persecution, been trafficked, faced political oppression or other sensitive situations, and may have considerable fears for their safety, or that of their family. Similarly, those using family reunion to physically reunite may be stuck in precarious situations trying to exit countries, desperate not to be discovered in an environment where digital surveillance is constantly on the rise.

Thus, protecting the data of those using RFL services is essential for the trust of individuals and communities who approach the FLN. It is more than a need to comply with legal and regulatory frameworks; it is core to people's

---

"Cyberattack on the Italian Red Cross on 18 January," accessed 12 May 2025, https://www.rodakorset.se/en/who-we-are/pressrum/roda-korset-berattar/cyberattack-on-italian-red-cross/#:~:text=What%20happened%3F,%2C%20locations%2C%20and%20contact%20information.

21 "Towards safer digital services: The CTA data breach one year on," accessed 12 May 2025, https://missingpersons.icrc.org/news-stories/towards-safer-digital-services-cta-data-breach-one-year.

22 The Missing Persons Digital Matching project has been piloting the use of algorithms to search the ICRC's, National Red Cross and Red Crescent Societies', and partners' databases (i.e. certain non-governmental organisations or international organisations). In line with established agreements, at the click of a button, the search engine flags a match for further investigation without accessing the whole of these databases. A human validation process is then made to verify the match and gain consent. It is now used for all ICRC delegations, piloted in five National Societies, and is being rolled out to other National Societies.

23 ICRC had planned to develop the use of facial recognition to increase matches. However, this project has not yet started.

safety and an embodiment of the principle of humanity. It is also a way to preserve impartiality, neutrality, and independence, which are increasingly under 'digital pressure' as data and technology have become core vectors of political, commercial, security, and military agendas.

While the FLN has had a long tradition of recognising the importance of keeping data about the people it works for confidential, the origins of data protection guidance and tools are more recent. In 2005–2006, a global mapping of the status of the FLN was undertaken by the ICRC and National Societies, which included an assessment of capacity covering the ICRC Central Tracing Agency's (CTA) capacity to act as coordinator and technical advisor for RFL services to National Societies.

The review concluded that while the CTA had experience of keeping data secure and confidential, the realities and wide variety of contexts in which National Societies operate meant that approaches to data protection were either not realistic or appropriate guidance was not available. It highlighted that parts of the FLN were not functioning well or did not exist, along with challenges for the Network in embracing technology.[24]

Thereafter, an Advisory Group, comprising 19 National Societies, the IFRC and the ICRC, and leaders of National Societies, created a global Restoring Family Links strategy, the first of its kind for the Movement. Data Protection was highlighted at 2.4.8, with the ICRC/CTA committing to:

> *Work for the development, by 2013, of common principles for RFL. Such principles would include common definitions, professional standards and ethical norms, compatible procedures and systems, the definition of target populations, specific aspects of RFL activities (e.g. child protection), data protection and needed coordination mechanisms.*[25]

A Strategy Implementation Group, composed of the ICRC, the IFRC, and National Societies from the four regions, was also established to support the implementation of the global RFL strategy and monitor progress.

In this context, and with the drafting of the European Union's General Data Protection Regulation (GDPR) having started, plus the emergence of other data protection regulations across the world, the need for common

24 Ralph Otto and Stéphane Jeannet, "Review of the ICRC and CTA capacity to act as Coordinator and Technical Advisor in Restoring Family Links (RFL) Activities with National Societies and Governments," ICRC, February 2007, ALNAP, accessed 26 May 2025, https://alnap.org/help-library/resources/review-of-the-icrc-and-cta-capacity-to-act-as-coordinator-and-technical-advisor-in/.

25 "Restoring family links strategy: including legal references, 2008–2018," ICRC, 32, https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0967.pdf.

principles for RFL in relation to data protection became a priority. Without them, entities of the FLN that were to become subject to the GDPR risked not being compliant with it and other applicable norms, or having the data flow between Europe and other parts of the world disrupted.

RFL Code of Conduct on Data Protection

Creation

The principle of universality, where all National Societies within the Movement have equal status and share equal responsibilities and duties in helping each other, is fundamental to RFL, as is the transfer of data cross-border between members of the FLN (and to third parties). Yet the myriad of laws and regulations internationally on data and its use make it complex to share data for the purely humanitarian purpose of reuniting families.

Global diversity in data protection has implications for RFL services. For example, some States have no specific national legislation, e.g. Afghanistan and Eritrea do not have a data privacy law or a data privacy authority.[26] Other States have adopted very strict laws on how organisations must protect data, such as Australia[27] and the UK.[28] However, operationally, the Afghan and Eritrean communities are significant users of RFL services, requiring the British Red Cross to send data to these contexts and/or other countries.

In response to the challenges arising from operating across differing legal jurisdictions, a single code of conduct for how data is managed in the FLN was envisioned – a common set of essential principles by which its members would function. This would, in theory, ensure the FLN was storing and transferring data in a way that keeps the protection of separated individuals at the heart of any processing, and assure other stakeholders of standards in data processing.

Thus, in late 2013, a working group, comprising the ICRC, the IFRC, the Red Cross EU Office and four National Societies, set about creating the RFL Code of Conduct on Data Protection. A series of meetings and consultations with National Societies culminated in the adoption of the Code in November 2015.[29] The Code sets out the minimum principles, commitments,

26 "Global Table of Countries with Data Privacy Laws, Treaties, or Conventions," World Privacy Forum, accessed 16 February 2025, https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/.

27 "Privacy," Attorney-General's Department, accessed 23 April 2025, https://www.ag.gov.au/rights-and-protections/privacy.

28 GDPR and Data Protection Act 1988, accessed 27 April 2025, https://www.legislation.gov.uk/eur/2016/679/contents and https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

29 RFL Code of Conduct on Data Protection Version 1.0 November 2015, accessed 11 April 2025, https://rcrcconference.org/app/uploads/2019/07/rfl-code-of-conduct.pdf.

and procedures that personnel of the ICRC, National Societies, and the IFRC need to comply with when processing RFL personal data. National Societies must still comply with their own national legislation, which takes precedence over the Code.

In recognition of the differing contexts and resources available to different National Societies, the Code was envisioned as a tool for supporting collaboration between different parts of the Movement, rather than as a legally binding enforcement tool. Within the FLN, there is a great range in the level of maturity in the area of data protection, and very different legal cultures, as well as different resources available and unique operational challenges, with many entities operating in volatile environments.

Furthermore, the spirit of the Movement is one of cooperation and partnership with a focus on capacity strengthening and solidarity, which is not fully aligned with the spirit of the GDPR's Chapter V transfer mechanism that focuses on enforceability and potential litigation for non-compliance.

Rather, the approach was pragmatic and cognisant of the practical realities of carrying out RFL humanitarian activities within conflict settings, refugee camps, or with minimal resources. An Application Group was created, led by the ICRC with National Societies from each of the four world regions. In addition, RFL Data Protection Focal Points were established in each National Society RFL unit. The Code was translated and made available in 16 languages:[30] English, Arabic, French, Spanish, Russian, Portuguese, German, Turkish, Farsi, Tamil, Sinhala, Croatian, Dari, Pashto, Romanian, and Serbian.

Integration into a Global Strategy for RFL

By 2019, a subsequent global strategy had been created, Restoring Family Links: Strategy for the International Red Cross and Red Crescent Movement 2020–2025[31] (recently extended to 2030[32]). Data protection features more prominently in this strategy with a dedicated workstream, Enabler 3 Protection of Individuals by Protecting their Personal Data.[33] National Societies and ICRC Delegations undertake annual self-assessment surveys on

30 However, when version 1.0 was replaced with version 2.0, all the translations of version 1.0 were removed. New translations of 2.0 are gradually being added. https://www.icrc.org/en/document/rfl-code-conduct.

31 "Restoring Family Links: Strategy for the International Red Cross and Red Crescent Movement 2020–2025 – Including Legal References," ICRC 2019, https://www.icrc.org/en/publication/4507-restoring-family-links-strategy-international-red-cross-and-red-crescent-movement.

32 "Resolution on extension of RFL global strategy to 2030," October 2024, accessed 3 March 2025, https://rcrcconference.org/app/uploads/2024/10/CoD24_R6-Res-RFL-EN.pdf.

33 Ibid., 49.

progress against data protection criteria, of which compliance with the RFL Code of Conduct on Data Protection is one.

Application of the Code

Implementation and Compliance

The RFL Code of Conduct on Data Protection Application Group comprises the ICRC, 18 National Societies from different regions, and the IFRC.[34] The Group has produced guidance such as an Information Notice template[35] and Guidance on data retention and data deletion in RFL.[36] Like the RFL Code of Conduct on Data Protection, the Guidance specifies that domestic data protection laws take precedence. Therein lies one of the challenges in implementing the Code, because a country that passes invasive laws linked to counter-terrorism, crime prevention, or immigration control purposes, for example, may naturally be at odds with the principles of the Code. This dilemma regarding the disclosure of personal data to authorities, which challenges the impartial, neutral, and independent humanitarian action of RFL, is highlighted in the Handbook on Data Protection in Humanitarian Action.[37] In order to deal with this issue, the International Conference[38] adopted a Resolution on RFL and Privacy, including data protection[39] in which it stressed the importance of Neutral, Impartial, Independent Humanitarian Action (NIIHA), trust, and a request that governments do not ask for data collected by RFL that would be used for purposes incompatible with the work of the Movement.

34 RFL Code of Conduct on Data Protection Application Group members list as at 4 January 2023.

35 Based on internal guidance of the Movement: *RFL Guideline, 12.01 Template & Information Notice* (not publicly available) Family Links Extranet (Family Links Network's internal Intranet), accessed 5 May 2025. https://icrc.sharepoint.com/sites/flextranet/SitePages/12.1-Template-and-Information-Notice.aspx

36 Based on internal guidance of the Movement: *Guidance on Data Retention and Data d=Deletion in Restoring Family Links* (not publicly available) RFL Family Links Extranet (Family Links Network's internal Intranet), accessed 3 March 2025.

37 Massimo Marelli ed., *Handbook on Data Protection in Humanitarian Action*, ICRC, 3rd edition, (Cambridge: Cambridge University Press, 2024): 3.7.1 54 & 55, accessed 6 May 2025, https://doi.org/10.1017/9781009414630.

38 The International Conference is where all components of the Movement and states that are party to the Geneva Conventions meet every four years to make commitments to joint action through the adoption of resolutions. See "Statutory Meetings – Power of humanity for further information and past resolutions," https://rcrcconference.org/.

39 "Resolution 4 – Restoring Family Links while respecting privacy, including as it relates to personal data protection – Statutory Meetings," accessed 26 May 2025, https://rcrcconference.org/about/reporting/33ic-resolution-4-restoring-family-links-while-respecting-privacy/. International Red Cross Red Crescent Movement Council of Delegates 2019.

Figures collected through annual monitoring and evaluation self-assessment surveys show a gradual positive trend of global improvement in data protection compliance against the Code.[40] But there remains a significant need for improvement. Based on the 2024 results, only 29% of National Societies and RFL units of ICRC Delegations are 'fully' or 'medium' compliant with the Code, with other RFL units working towards this.

Monitoring indicators that National Societies and ICRC Delegations find the most difficult to achieve are:

- systematic use of encrypted and secure communication means for the external sharing of personal data with other third parties;
- systematic use of encrypted and secure communication means for the external[41] sharing of personal data internally (e.g. secure and encrypted institutional email account);

Whilst the FLN has a Secure File Exchange for within the Movement, and interoperability within its casework management tool, securely communicating between non-Movement partners can be more complicated. Each National Society may have a variety of third parties with which they need to interact and share data (some of which they may be unaware of due to the very nature of digital infrastructure and data flows[42]). This variety, coupled with the current financial constraints within the ICRC including a reduction in resources for digital development in RFL,[43] means that the issue of encryption and sharing data securely externally remains a continued challenge in implementing the Code.

For example, in order to meet the key indicator within the data protection section of the RFL global strategy, the British Red Cross looked to use its

40 Key monitoring indicators include the extent to which the Code is integrated into training, whether RFL staff have institutional emails, whether systematic use of encrypted and secure communication is in place, and whether there are procedures within operations for secure data management.

41 "External" in this monitoring indicator refers to the sharing of data between different parts of a National Society, e.g. between branches and headquarters.

42 Giulio Coppi, *Mapping Humanitarian Tech: Exposing protection gaps in digital transformation programmes*, Access Now, February 2024, https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf.

43 In March 2023, the ICRC announced substantial cuts to its operations. "ICRC to resize global footprint, maximizing reduced resources in era of declining aid budgets," accessed 27 May 2025, https://www.icrc.org/en/document/annual-report-2022. This led in 2023 and 2024 to a significant reduction in staff and resources, including a reduction of around 4,500 personnel. In 2022, the ICRC had 22,562 staff: "Annual Report 2022 | ICRC," and as at 10 June 2025, this had reduced to approximately 18,000 personnel: "Meet our colleagues". This has led to a reduction in the ICRC's capacity to sustain digital innovation for RFL, and no new tools for RFL are planned.

organisational encryption tool to share the personal data of those using the family reunion travel assistance service between the British Red Cross and its partner, the International Organisation for Migration (IOM) UK. However, the encryption tool, due to its data protection by design functionality, was not conducive to urgent humanitarian work with partners abroad.

To overcome this, the British Red Cross and IOM UK established alternative arrangements for the secure transfer of cases. Once such cases were received, the IOM was then able to share them with overseas missions via their internal encrypted systems.

Furthermore, there may be contextual challenges that make it difficult for National Societies to fully implement the Code. For example, in South Sudan there is no national law on data protection, so whilst the Code has been helpful as a guide, it can be difficult when third parties do not treat the data in the same way because of the absence of a specific law.

In addition, understanding of data protection principles and literacy within the general population is a factor, as well as language. In South Sudan, there are 64 tribes with 64 languages, as well as the main languages of Arabic and English. The South Sudan Red Cross has volunteers who visit people to explain in the relevant language how their data will be used. This, coupled with the challenges of keeping physical resources secure when operating in a conflict situation where offices may be broken into, means significant resources are needed to collect, enable informed consent, and store data. With staff turnover, the need for ongoing training – including peer-to-peer training with a National Society or ICRC Delegation fully compliant with the Code – has been highlighted as important for enabling the implementation of the Code.[44]

It is essential that the Movement and States work to ensure National Societies have the independence, resources, and technical ability to implement the Code. Of particular importance is the need for the centralised digital tools used by the FLN to be adequate in respect of cybersecurity and user-friendly to encourage uptake and proper use.

Legal Bases

The original RFL Code set out the basic principles for data processing and data controller commitments, including a specified purpose, lawful and fair processing (the legal bases), and data processing commitments such as fairness, transparency, data minimisation, accuracy, integrity and confidentiality, and the rights of data subjects. In regard to legal bases, the Code specified

44 Interview with David Owot, RFL Lead, and Emmanuel Lopia, Data Protection Officer, South Sudan Red Cross, 10 April 2025.

consent as the preferred legal basis, with an emphasis on informed consent, and the use of other legal bases when consent was not possible.

However, there are some inherent difficulties with the original, recommended legal basis of consent due to the nature of tracing and the complexity of understanding the risks attached to digital technologies. Users are required to give detailed (and sometimes sensitive) information about a missing relative to initiate a search. This data is inevitably processed without the consent of that relative. Tracing cases, thus, requires a different legal basis, such as public interest. In the context of the Movement's work on RFL, the public interest can relate to the implementation of a humanitarian mandate to restore family links as set out in the Geneva Conventions Additional Protocols, the statutes of the Movement, International Conference resolutions, and domestic laws (including national Red Cross Laws).

There is also a more general question around whether one can ever obtain truly informed consent from the person looking for their loved one due to the power imbalance between the data subject and the data controller and the emotional bias from having lost a relative. If an organisation has the power to find someone's child, which parent will not agree to almost anything in order for the National Society to find them? In consequence, consent is not a completely reliable legal basis on which to process the data.

Moreover, the challenging context of RFL means that the notion of informed consent remains problematic. The RFL process is a complex undertaking and it is hard to fully explain the steps taken and risks involved. The consent may take place with the British Red Cross in the UK while the search is conducted by the ICRC or another National Society in a different country in a context that is constantly changing. Thus, families will have to partially rely on the Movement's 'do no harm'[45] assessments, and it is essential that RFL operates with people with lived experience who can advise on the best communication methods and approaches.

Nevertheless, despite the limits to consent, this does not mean the FLN will stop its long tradition of seeking feedback and agreement from the data subject. Providing as much information as possible about the proposed activities and processing of data is an important part of building trust, as is applying the 'do no harm' approach in obtaining agreement from the enquirer on how their data will be used and understanding the potential implications of that for them and their missing family member.

45 Mary B. Anderson, *Do No Harm: How Aid Can Support Peace or War* (Boulder: Lynne Rienner, 1999).

Resolutions of the International Conferences of the Red Cross and Red Crescent

To further reinforce key elements of data protection in humanitarian action, further resolutions have been adopted, the most relevant of which is *Restoring Family Links while respecting privacy, including as it relates to personal data protection* (2019).[46] This resolution supports the interpretation of data protection requirements for RFL contained within the Code. It reaffirms the respective mandates of the Movement's components in RFL, such as the auxiliary role of National Societies to their public authorities in the humanitarian field, and calls upon States to take measures to prevent people going missing and to clarify their fate. Importantly, it sets out the commitments of States and the FLN to collaborate in favour of separated families, recognising the Movement's need to process and transfer personal data for exclusively humanitarian purposes, and the critical flow of data across borders, highlighting the Code.[47] The resolution also recognises the difficulty in obtaining informed consent.

In addition, it highlights the exclusively humanitarian purpose of RFL and explicitly asks States not to request or use data that has been collected in the course of RFL for purposes that are not compatible with the Movement's humanitarian mission.

> *11. urges* States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement, and in conformity with Article 2, including paragraph 5 thereof, of the Statutes of the Movement, or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of RFL services;

However, despite the commitment made in this resolution, the FLN continues to be challenged by requests from States and other actors for RFL data for non-RFL purposes, sometimes without any humanitarian purpose, or for quite the opposite purpose. This includes requests for personal data for immigration control, counter-terrorism purposes, and under mechanisms linked to criminal justice, e.g. DNA data collected for the purpose of clarifying the fate of a family member being subject to checks against criminal databases. This reinforces the need to strengthen international understanding, acceptance,

46 *Restoring Family Links while respecting privacy, including as it relates to personal data protection (2019)*, 4.11, accessed 3 March 2025, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf. International Red Cross Red Crescent Movement Council of Delegates 2019.

47 *Restoring Family Links*. 4.9.

and support by all to ensure exclusive humanitarian use of data collected by the Movement.

Particular risks have been observed where RFL data is sought to be used as evidence in asylum cases. People's decisions to use (or not to use) the British Red Cross's RFL services have been cited in determination letters and asylum appeal refusals despite considerable efforts by the British Red Cross to explain to legal advisors, government, and the judiciary the negative impact such citations have on the service. The instrumentalisation of the service in this manner distorts its use and prevents people who are looking for their loved ones from using it, taking up capacity that should be otherwise directed solely for the purposes of RFL in managing requests. As well as absorbing capacity, it undermines user trust and violates the need to respect the ability of humanitarian organisations to operate in line with their humanitarian mandate and principles. A continuous dialogue with authorities and other stakeholders who seek to use information linked to RFL services is, therefore, required to prevent data collected for this humanitarian purpose from being misused.

Updating the Code

The Code was updated by a Movement working group in 2024[48] to maintain its relevance in the changing regulatory environment worldwide and to reaffirm the FLN's commitment to protecting the data of those it serves.

The main aim of the Code remains the same, setting out the standards expected to be followed by the FLN on data protection. However, there are some key changes.

Firstly, there is a change in the recommended legal basis for the FLN. Where previously the recommended preferred basis was consent, there was an acknowledgement in the International Conference Resolution 4/2019[49] of the challenges of relying on consent for the provision of RFL services. In the updated Code, consent is one of the possible but not preferred options. Like the previous version, it acknowledges that RFL services can rely on other legal bases such as public interest, which is considered fundamental for RFL activities, or vital interest. Specifically, in paragraph 5.1 it states: "In accordance with section 2.2.1, public interest is the preferred legal basis for the publication of personal data." Accompanying this are instructions for National Societies to check the applicability of the public interest legal basis according to their national laws.

48 RFL Code of Conduct on Data Protection Version 2.0, 2024, accessed 11 April 2025.

49 *Restoring Family Links while respecting privacy, including as it relates to personal data protection (2019)*, 6.

An early example of this approach, which predates the Code, resulted in the French Red Cross receiving an 'authorisation' from their data authorities, the *Commission Nationale de l'Informatique et des Libertés* (CNIL) in 2012, which recognised that RFL activities are in the public interest and allows data to be sent out of the European Union:[50]

> Data may be transferred to ICRC delegations or to Red Cross National Societies located outside the European Union, *insofar as such transfers are necessary for the protection of human life and the public interest*, in accordance with Articles 69(1) and 69(2) of the amended Law of 6 January 1978.[51] (emphasis added).

A French law was later adopted in December 2016 which now permits the French Red Cross to have access, for RFL purposes, to personal data held by certain French public bodies. Notably, under article 2, the law recognises that RFL is considered in the 'general interest'.[52]

Case Example – Checking Applicability of Public Interest as a Legal Basis

According to 2.2.1 of the 2024 Code of Conduct on Data Protection, before seeking to rely on the public interest, "National Societies should first check whether their domestic law would allow them to rely on it as a legal basis for data processing."

Whilst UK legislation on Data Protection can be interpreted as including humanitarian activities as within the scope of the public interest, it does not do so explicitly. Consequently, the British Red Cross decided to approach its public authorities to seek clarification on the interpretation of the relevant legal rules.

In 2024, the British Red Cross provided a paper to the UK public authorities containing a detailed legal rationale explaining how current UK law theoretically permits the British Red Cross to rely upon the public interest legal basis. The paper included arguments rooted in both domestic and international law, as well as the Movement's special features, e.g. the auxiliary role. The British Red Cross subsequently received confirmation which recognised that it was 'plausible' for the British Red Cross to rely on the public

50 Letter to French Red Cross from Isabelle Falque-Pierrotin of the CNIL, 24 May 2012, DELIBERATION n°2012-161 du 24 mai 2012 – Légifrance. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000026241772/

51 Author's own translation.

52 Law No. 2016–1919 of 29 December 2016, concerning the exercise by the French Red Cross of its statutory mission to restore family links, accessed 27 May 2025, https://www.legifrance.gouv.fr/eli/loi/2016/12/29/MAEX1613781L/jo/texte.

interest when processing personal data for the purposes of RFL activities. The response, nevertheless, emphasised that where possible, consent should be the principal legal basis relied upon.

Another key change, taking into account learning from the data breach of 2022,[53] was a focus on what components of the Movement must do in the event of a breach, their responsibility to inform and to carry out risk assessments, and the Central Tracing Agency's role in coordinating responses that affect caseloads shared among FLN members.

With regard to data transfer, in the updated Code there is a clear indication that a Data Sharing Agreement (DSA) is not needed between members of the FLN for RFL activities, but rather a reinforcement of the idea that there is an obligation to inform those using RFL services through the Information Notice[54] or equivalent about possible transfers to places that may not have the same level of data protection. In addition, there is more guidance on how to complete a Data Protection Impact Assessment (DPIA) and advice that it should include the Data Protection Focal Point from the onset of any new partnership or tool to transfer data.

The updated Code outlines how this Focal Point should have a strong background in RFL and an understanding of data protection principles and obligations. It also emphasises the importance of developing a network with other Focal Points to create a community of practice across the FLN.

The newly updated Code also highlights data deletion and the importance of the relationship with the data subject in this regard, as well as instructions for what needs to be done when receiving a right to erasure request. It also adds a definition of sensitive data and its use depending on the context.

Challenges have been identified in making the complex legal concepts and technical language of the Code understandable and easily digestible for RFL practitioners on the ground. Recognising the enormous pressure RFL service volunteers and staff are under due to caseload demands and/or the fact of operating in conflict, disasters, or other volatile settings, steps have been taken to develop additional user-friendly, efficient, and simple tools to improve understanding and compliance with the Code. This includes an

53 "Cyber security incident: How could it affect me?" ICRC Blog June 2022, accessed 5 May 2025, https://www.icrc.org/en/document/cyber-security-how-it-affect-me.

54 Based on internal guidance of the Movement: 12.01 Template and Information Notice (not publicly available) RFL Family Links Extranet (Family Links Network's internal Intranet), accessed 3 March 2025.

online DPIA template,[55] a one-page factsheet,[56] an animation,[57] and even an RFL Code of Conduct board game,[58] to introduce the principles. However, operationalising the Code on a rolling basis remains a key ongoing challenge. The following example illustrates the importance of training and some of the obstacles to implementing the Code:

Case Example Ecuador Red Cross

"In my case I could better understand this document [Code of Conduct] after I went on the course at Maastricht University – Data Protection Officer (DPO)[59] and it is better to disseminate with my coworkers and in the field and the volunteers".[60]

Following the data breach of 2022 and the adoption of Ecuador's first dedicated law on data protection, the Ecuador Red Cross RFL unit had an in-depth focus on the RFL Code of Conduct. "We decide to share some exercises, to remember about the code of conduct, but with some simulations, some drills, inviting volunteers from the provinces".[61]

The RFL lead for the Ecuador Red Cross also planned to do some exercises to raise personnel's awareness of the updated 2024 Code of Conduct. However, widespread flooding impacted capacity and has made ongoing training challenging.

As well as the challenges of natural disasters and emergencies, the Ecuador Red Cross has to contend with electricity outages that can make using some of the digital data protection tools, such as Family Links ANSWERS and

55 Family Links Network Code of Conduct for Data Protection Template for Data Protection Impact Assessment (DPIA) dpia-template.pdf ICRC, accessed 2 May 2025, https://www.icrc.org/sites/default/files/document/file_list/dpia-template.pdf.

56 "Data Protection: Key Principles for Personnel of the Family Links Network," accessed 12 May 2025 https://shop.icrc.org/data-protection-key-principles-for-personnel-of-the-family-links-network-pdf-en.html <u></u>Available in English, French, Arabic, Spanish, Portuguese, and Russian.

57 A generic animation was created by the RFL Code of Conduct on Data Protection Application Group, which National Societies could then adapt with their own language to explain the principles of how the Family Links Network processes data. *We help trace relatives separated by crises | Restoring Family Links*, British Red Cross accessed 22 April 2025, https://www.youtube.com/watch?v=TTaqcw-YgLI.

58 "RFL Data Protection Board Game," ICRC, accessed 5 May 2025, https://shop.icrc.org/rfl-data-protection-board-game-print-en.html.

59 *Data Protection Officer (DPO) Humanitarian Action Certification,*Maastricht University, accessed 7 May 2025, https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-humanitarian-action-certification.

60 "Interview with María Fernanda Carrera Rodríguez, RFL lead for Ecuador Red Cross," 6 May 2025.

61 "Interview with María Fernanda Carrera Rodríguez, RFL lead for Ecuador Red Cross," 6 May 2025.

secure file exchange, difficult. Another aspect is that the national data protection law has not been in force long, so there is a lack of understanding of data protection among some agencies and local organisations. As a result, other organisations have requested the personal data that the RFL team holds, leading to the latter having to explain data protection and the way the RFL service works.

Conclusion

Data Protection continues to be core to the provision of RFL services. The introduction of the RFL Code of Conduct, whilst challenging to implement due to the variety of contexts in which RFL units operate – including in conflict, in countries with a lack of national data protection legislation, and/or in places with varying levels of infrastructure – has been valuable in providing a guiding set of principles for the FLN. It has also galvanised a 'whole-network' approach to data protection issues, creating more uniformity in aspects such as information notices, secure file exchange, and digital tools.

Nevertheless, more remains to be done to tackle the challenges presented throughout this chapter. This includes working to provide continuous training, guidance, and peer-to-peer support to National Societies, alongside working with people with lived experience to ensure materials and communications are appropriate and enable people to make informed choices regarding the use of personal data. Additionally, investment in digital tools and innovation needs to be prioritised to ensure tools are relevant, user-friendly, and reduce the risk of cyber-attacks or exploitation.

Finally, continuous dialogue with authorities and other stakeholders is needed to explain RFL services and the Code to counter both the absence of data protection knowledge or laws, and risks of the misuse of RFL data for non-humanitarian purposes.

Having a loved one missing is torture enough, without the data about them being misused to add to their suffering.

13

BY THE BOOK, BEYOND, AND BACKWARDS?

Ethical Considerations on the 2022 Data Breach Affecting the Family Links Network of the Red Cross and Red Crescent Movement

Natalie Klein-Kelly[1]

Was the 2022 breach of a particular set of data platforms of the Red Cross and Red Crescent (hereafter the Movement) the "catastrophic data breach" that would, it was claimed, make humanitarian organisations and their donors "sit up and listen" to the need to understand the link between technological developments, digitalisation, and the need for data protection?[2]

The breach was discovered on 18 January 2022. Within 24 hours of the breach's discovery, the International Committee of the Red Cross (ICRC) set the tone of transparency by going public about the incident, with a first announcement on 19 January, with a – so far – final communiqué on the topic in June 2022. At the time, the ICRC stressed that it had to be assumed that the full data set, containing the personal data of more than 515,000 data subjects, had been breached, viewed, and potentially downloaded in full.[3]

Even if no data was deleted or altered, and no evidence of use of this data has been found to date, the incident met the Movement's Family Links

1 The views expressed in this article are those of the author writing in a personal capacity. While the content refers to specific events within the ICRC, the interpretations and opinions presented do not reflect the official position or views of the ICRC. The article is intended to offer a personal perspective and should not be taken as an institutional statement.

2 Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and 'Big Data'," *International Review of the Red Cross* 99, no. 1 (2017): 209, https://doi.org/10.1017/S1816383117000637.

3 "Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people," ICRC, 19 January 2022, https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people. "Cyber attack on ICRC: What we know," ICRC, 16 February 2022, https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

DOI: 10.4324/9781003650164-19

Network's (FLN) definition of a data breach.[4] In line with domestic legislation in many of the countries where the data subjects resided, the FLN proceeded to arrange notifications, as also required by the Restoring Family Links (RFL) Code of Conduct (hereafter the Code), based on risk assessments to understand whether the breach was deemed likely to result in high risks to data subjects and to verify that there was no reason why notifications should not be issued. This 'by the book' response was followed by an additional, second exercise by the FLN, proposed by the ICRC, to centrally record risk assessments and mitigation actions using a proposed methodology, thus, in various ways, going 'beyond' the regular response. This 'additional' exercise, its results, and significance are at the centre of this chapter. Other relevant aspects of the response to the data hack, including how the functionalities of the breached platform were rebuilt, what was done to analyse and address the data security of this and other platforms used by the Movement, and how public communication decisions were taken, will not be covered.

To understand the seriousness of the breach, it is necessary to take a step back and look at the humanitarian activity it relates to. The collection, processing, and usage of personal data is at the core of RFL work, one of the first operational activities of the nascent Movement dating back to the 19th century.[5] In recognition of the humanity of each individual, in the form of a unique name and identity, RFL is designed to safeguard this human identity, administratively and in its connections to other people: i.e. to communities and families.[6] To effectively restore family links, an activity which generally has cross-border elements and involves more than one entity of the FLN, personal data on individuals is collected. Two or more data subjects are interconnected – i.e. typically belonging to the same family. This data is held, sometimes for decades, for the benefit of those concerned, but also for their descendants.[7] Today, this activity has grown into a well-established and expansive activity of the Movement, with – at the point of the data breach – close to 150 National Societies and 80 ICRC Delegations involved, holding personal data on millions of persons, some of which was stored on the breached data platform.

4 Restoring Family Links, *Code of Conduct on Data Protection*, version 2 (ICRC, 2024), 8, https://www.icrc.org/en/document/rfl-code-conduct.

5 Gradimir Djurovic, *L'Agence Centrale de Recherches du Comité International de la Croix-Rouge. Activité du CICR en vue du soulagement des souffrances morales des victimes de guerre* (Institut Henry Dunant, 1981).

6 For the importance of human identity: Nathalie Deffenbaugh, "De-dehumanization: Practicing humanity," *International Review of the Red Cross* 106, no. 925 (2024): 60–61, https://doi.org/10.1017/S1816383124000079.

7 One of the post-World War II ex-ICRC tracing services centres receives 20,000 information requests on individuals each year, over half a century later: Arolsen Archives, *Jahresbericht 2023* (Bad Arolsen, 2024), https://arolsen-archives.org/story/jahresbericht-2023/.

The data breached in 2022 can thus be understood as "lists of interconnected names" that allow the tracking and tracing of those at risk of disappearance, or of those with whom contact has already been lost.[8] The data is not the by-product of humanitarian services collected for the sake of processes, efficiency, or accountability. Rather, holding and using the data, finding connections between them, and keeping the data safe for future use by those who provided it, is *the* humanitarian service provided by the FLN.

In the 2000s, both the ICRC and certain National Societies increasingly understood that new and enhanced ways to manage, but also to protect, this data would be needed in order to ensure respect for the rights, dignity, and safety of affected persons. How to ensure compliance with emerging legal data protection requirements had to be considered, as well as how to retain the trust of beneficiaries in view of the heightened vulnerability of electronic data, also through its increased centralisation. As described by Emily Knox,[9] this led to both reflections on, and codifications of, how the protection of this data needed to be managed in the following decade, and included what should be done if a breach occurred. A Code of Conduct specifically for RFL work was developed, as well as several other guidelines, both ICRC-specific and for the humanitarian sector in general.[10]

It can therefore be argued that the FLN had prepared for the event of a data breach by the time the 2022 event occurred. Personal data in settings where humanitarian organisations operate, including the FLN, may include (very) sensitive data.[11] At first glance, what is collected and held may seem comparatively unproblematic, if breached: names and basic information such as date of birth or patronym, together with contact details including, typically, physical locations, and – for sought persons – last known addresses. Financial data, health data, biometric data, or passwords are typically not included, as they are not relevant to tracing people. For example, the Movement's services are free of charge and thus do not require financial data. However, humanitarian organisations operate in situations where there may be other complex risk factors. Sensitive data such as racial or ethnic origins, or political or religious

8 Kristin Bergtora Sandvik, *Humanitarian Extractivism: The Digital Transformation of Aid* (Manchester University Press, 2023), 79.

9 Chapter 11, "Data protection in the framework of Restoring Family Links humanitarian activities: Code of conduct, resolutions, and data breaches".

10 Family Links Network, *Code of Conduct*; ICRC, "ICRC Rules on Personal Data Protection" (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html; Massimo Marelli, 3rd ed., *Handbook on Data Protection in Humanitarian Action* (Cambridge University Press, 2024).

11 Global Privacy Assembly, *Resolution on Privacy and International Humanitarian Action* (37th International Conference of Data Protection and Privacy Commissioners, 2017), https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf, Point 4.

affiliations, may be revealed inadvertently, for example a name itself may be an indication of tribe or ethnicity.[12] As Dogu Han Buyukyagcioglu explains,[13] such realities and complexities specific to humanitarian organisations and their activities have influenced and matured the codification, practice, and application of data protection principles in this sector over the past decade.

Ethical perspectives are important here, as are practical and legal considerations. As with medical ethics, complex values govern decision-making regarding individuals in humanitarian action. This includes a recognition of the autonomy of patients or beneficiaries who should be helped to reach their own decisions, the principle of beneficence, to promote what is best for the individual concerned, and that of non-maleficence.[14] In data protection, and specifically in the context of data breach handling, these values can be related to the recognition of the need to allow data subjects to take their own action by being notified about the danger – i.e. the breach – while balancing the principle of 'do no harm' and the ultimate objective of 'doing good'. Therefore, difficult questions surrounding the reasons why personal data should be protected, in each situation and for each individual concerned, and who should judge the level of risk, must be asked. Perception and understanding of risks may differ between countries in the global context in which humanitarian organisations such as the FLN operate.

Again from an ethical perspective, protecting data and dealing with a data breach responsibly is not really a choice in the humanitarian sector, considering how its mission and identity are centred on 'doing good' and not 'harm'. Meeting legal and regulatory obligations may not be sufficient. A catastrophic event in this regard could, indeed, be detrimental to "humanitarian action more generally", as the Movement itself recognised in 2019, as it could destroy the broad trust humanitarian organisations rely on to operate.[15] The response to the 2022 data hack can be regarded as part of this responsibility.[16]

12 Art. 9 (1), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *OJ L* 119/1 (2016).

13 Chapter 14, "Growing data protection maturity in humanitarian action: changes in understanding of key concepts in theory and in practice".

14 Michael Dunn and Tony Hope, *Medical Ethics: A very short Introduction* (Oxford University Press, 2018), 30.

15 Point 18 in *Resolution: Restoring Family Links While Respecting Privacy, including as it Relates to Personal Data Protection* (33rd International Conference of the Red Cross Red Crescent Movement, 2019), https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

16 The following two sections rely on ICRC internal information, mainly the *Report on the Risk Assessments in Relation to the Data Breach Carried out by the Family Links Network* (ICRC, 2022) cited with permission of the ICRC, and 'practitioner views' including those of the author as ICRC staff at the time of the breach.

The 'By the Book' Response by the FLN

A closer look at the guidelines and the Code mentioned above shows that transparency and notification of data subjects are central pillars of a 'by the book' response: "the data controller notifies the data subject of the occurrence of a personal data breach if it is likely to affect the rights and freedoms of the data subject […] to minimize risks of negative effects on the data subject".[17] ICRC Rules also specify that data subjects have a right to information.[18] In addition, amongst the National Societies specifically affected as data controllers, many were bound by their domestic data protection laws to notify both data protection authorities and data subjects.

Accordingly, the various affected FLN entities, National Societies, and ICRC Delegations embarked on individual notifications to data subjects, following the necessary risk assessments. Notifications were pursued through various means, according to available options and in line with each Movement component's usual ways of contacting beneficiaries: a choice of text messages, emails, phone calls, and in-person meetings. In parallel, this was accompanied by proactive and reactive public messaging, dedicated hotlines, and distribution of specific information materials. Approaches were combined if deemed necessary and feasible. For example, in some instances, data subjects were notified through a phone call, followed by an email offering further information and details of hotlines that were available to data subjects, as needed, for any further advice or discussions.

Not *every* data subject needed to be reached, and, indeed, not every data subject was reached. For a start, a significant number of people were not contactable using the available contact information, which was to be expected as some cases had been dormant for several years by the time of the breach. For others, a conscious choice was made not to notify for one of two reasons, following the necessary risk assessments. No notification may have taken place if, first, the required effort to notify was deemed disproportionate to the assessed risks involved, or, second, approaching the data subject was considered to carry significant other risks for the data subjects, endangering them further, or causing distress. Such secondary risks generally arose from security conditions and specific situations beneficiaries were exposed to – namely, situations of armed conflict or other emergencies. Both factors – disproportionate efforts

17 Family Links Network, *Code of Conduct*, Point 2.3.8 (2015 version). The Code was updated in 2025, where the threshold for notification was increased, i.e. a breach must cause a significant risk for notification.

18 ICRC, *Rules on Data Protection*, Art. 20.

and avoidance of harmful secondary effects – are explicitly acknowledged in the guidance on dealing with data breaches as grounds for not notifying.[19]

Practical issues encountered included the fact that not all notifications were made within the timeframes required by domestic legal frameworks, due to complexities in notifying 'people on the move' whose contact details frequently change, and the time needed for reflection and decision-making on the above-mentioned secondary risks. Such issues arose despite very significant efforts and endeavours to try and reach data subjects, including, in some cases, volunteers travelling to remote areas to personally notify them. One such effort took place in Zimbabwe, where an ICRC staff member personally informed a data subject about the breach and found that even explaining notions such as a "cyber attack" can be difficult in communities that may be unfamiliar with such risks.[20]

In addition, different FLN components required time to coordinate and agree on who would perform the notification to data subjects held by two or more National Societies or ICRC Delegations.

The reactions of both beneficiaries and authorities to the notifications were generally reported as 'muted', in the sense of an absence of a vocal or emotional reaction, or in fact, no reaction at all. Data protection authorities and other authorities either acknowledged the notification with a degree of appreciation or showed general indifference. Individual data subjects generally 'took note'. Only very limited numbers of beneficiaries showed stronger concerns, with a "tiny group" of data deletion requests. Most beneficiaries asked for the FLN to resume its services and enquired whether their relatives had been found. Such somewhat unconcerned reactions to data breaches are not unusual, also in the commercial sector.[21]

While maybe daunting at first, time-consuming, and certainly not effortless, the way the FLN applied the available guidance shows that it can be done 'by the book', even for a serious data breach concerning data subjects and authorities in over one hundred countries. One could even argue that

19 ICRC, *Rules on Data Protection*, Art. 7; Family Links Network, *Code of Conduct*, Point 2.3.8.

20 This moment was captured in a screenshot from a social media post by Marie-Astrid Blondieux (2022), showing ICRC staff member Pamela Mhlanga notifying data subject Melody Chikenyere. The staff member later noted that the information was received with appreciation and contributed to building trust with the community, despite the inherent challenges of communicating such risks.

21 Due to costs associated with protective measures, optimism bias, a false sense of security, or a tendency to delay action until harm has occurred; Yixin Zou et al., "'I've Got Nothing to Lose': Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach," *Fourteenth Symposium on Usable Privacy and Security*, edited by Mary Ellen Zurko and Heather Richter Lipford (USENIX Association, 2018), https://www.usenix.org/conference/soups2018/presentation/zou.

the available humanitarian sector-specific data protection principles and requirements provided the sector with a way to act that appears to have been both acceptable to, and accepted by, the humanitarian practitioners, relevant authorities, and beneficiaries. A key factor here was the recognition in the available guidance of the specificities of the situations and constellations found in the humanitarian sector, allowing for exceptions to the general rule of notifications in recognition of the complex situations humanitarian organisations may be operating in.

The Additional Protection Risks Assessment Exercise – Going 'Beyond the Book'

While this could have been the end of the FLN's response to the data breach from a data protection point of view, the Central Tracing Agency (CTA) of the ICRC decided to move forward with an additional exercise, effectively and explicitly going 'beyond' what may have been legally mandatory or foreseen under the Code: an additional round of recording and reporting of risk assessments and of reflections on possible mitigation activities. Insofar as the methodology differed, some risk assessments may have had to be re-done in this second in-depth exercise to, for example, consider data subjects whose data was not breached.

A first reason for this decision was the concern that beneficiaries of the RFL services whose data was not processed through the hacked tools, or beneficiaries of other Movement services, might erroneously believe that their data was also breached. Such beneficiaries should be informed that their data was *not* breached, to prevent any potentially unnecessary but harmful mitigation action on their side, while using this opportunity to discuss the reality of the possibility of data breaches affecting them in the future. Second, it was felt that decisions not to notify, due to disproportionate efforts or harmful secondary effects, should also be recorded and reported centrally for each caseload, even if the risk assessments were already well reflected, justified, and documented in the context of the initial 'by the book' response. Third, the CTA wanted to specifically encourage broader mitigation action beyond individual notifications that are typically the focus of data protection rules, explicitly including community-based approaches and notifications.

Ethically, these motivations link to different values. First, there is the overarching 'do no harm' principle, acknowledged as central to the aid sector for decades, which may require double- and triple-checking that no preventable harm was done.[22] Second, data subject notifications and transparency towards

22 Wolfgang Jamann, "Do not harm. *Humanitäre Hilfe in Konfliktsituationen*," *Handbuch Humanitäre Hilfe*, edited by Jürgen Lieser and Dennis Dijkzeul (Springer, 2013).

all beneficiaries on data breaches are ethically important, as they recognise the agency of the affected and allow for a key role in the mitigation of risks.[23] Finally, the additional efforts to assess risks link to the principle of 'appropriate care and attention', including for accountability, that must be taken in all engagements in the aid sector.[24]

Thus, in early February 2022, the CTA presented the need for this additional exercise to centrally record, report, and potentially re-do, with a certain proposed methodology, the risk and mitigation assessments to the nearly three hundred FLN components active in RFL services at the time. A methodology for the exercise was proposed, and feedback on its completion and information on additional mitigation actions undertaken was requested. Seventy-nine ICRC Delegations and 149 Red Cross and Red Crescent National Societies, from all continents, participated and provided this feedback by mid-2022, representing 79% of all entities involved in RFL activities at this time.

National Societies and ICRC Delegations were asked to, first, group all individual tracing cases into caseloads from the perspective of implied risks. For example, cases related to conflict settings could be presumed to be exposed to different risks than cases related to natural disasters. Caseloads could be of significantly different sizes, ranging from tens of thousands to hundreds or even only scores of cases. In view of the Movement's ignorance of the actors behind the data breach, it was advised to not primarily consider the likelihood of the identified risks, but, rather, to focus on the potential severity of risks when considering necessary mitigation action.

For each caseload, three categories of risk were to be considered, with the possibility of all three categories applying to the same caseload. The first category of risks focused on potential criminal use of the data for the purpose of financial gain: i.e. extortion or phishing attempts. Second, the consequences of a public leak were considered: would beneficiaries face stigmatisation or discrimination if this happened? A third category was reserved for reflections on risks for specific groups of individuals, should their data have been the actual target of the actors behind the data breach. Based on these assessments, which also included space to reflect on potential secondary risks of notifications and to mention planned or completed mitigation action, a 'caseload record sheet' was to be sent back to the CTA.

A significant majority of the National Societies and ICRC Delegations compiled and returned such record sheets. Over 550 sheets were received by the time the reporting was wrapped up in the summer of 2022. Some

23 Also called 'stewardship principles' by Hugo Slim, *Humanitarian Ethics. A Guide to the Morality of Aid in War and Disaster* (Hurst and Company, 2015).

24 Christopher D. Wraight, *The Ethics of Trade and Aid. Development, Charity or Waste?* (Continuum International, 2011), 130.

FLN components grouped all their cases into one caseload and provided one record sheet in response, while others used up to ten such sheets, due to being involved in tracing activities related to different conflicts, disasters, or other emergencies which implied very different risk scenarios per caseload.

The risk most often identified for caseloads was potential criminal use, specifically mentioned in 63% of all record sheets received. Related risks were considered the least severe of the three categories. Extortion of people in vulnerable positions, also by people pretending to be from the Movement, is indeed a recurring risk.[25] At the same time, beneficiaries of FLN services are more likely than not to have limited (financial) resources, making them somewhat unattractive for larger financial crime. Next, 58% of record sheets considered publication of the data as a potential risk to data subjects, with mixed assessments of severity. Borrowing from a typology of harmful effects in social media, publishing names and identities can indeed bring severe consequences, even risks to life and wellbeing, as well as potentially less severe ones, such as risks to economic or cultural wellbeing and harm to social inclusion.[26] The most severe, but also the least often identified, risks were recorded related to the third category: the danger that the data breach specifically targeted a particular caseload. 43% of record sheets reflected on this risk, typically concerning smaller caseloads.

Regardless of this specific data hack, two specific scenarios have been mentioned in related academic literature where potential serious risks may develop, which can be considered here as general examples. The first relates to the tracking of undocumented migrants. It has been argued elsewhere that data on the identity of persons may be particularly vulnerable in situations of migration and resettlement, where there may be an interest in hiding identities.[27] This is augmented in the second specific example where entities may be seeking information on those who have fled and sought refuge elsewhere for protection. Here, having contacted the FLN for help to contact family members elsewhere could reveal current locations to States seeking to track and trace such individuals themselves.[28] Maybe in view of this risk, the Movement

25 "Warning: Scams and false claims misusing the ICRC's name," ICRC, accessed 10 May 2025, https://www.icrc.org/en/article/warning-scams-and-false-claims-misusing-ICRC-name.

26 Bailey Ulbricht and Joelle Rizk, "How harmful information on social media impacts people affected by armed conflict: A typology of harms," *International Review of the Red Cross* 106, no. 926 (2024), https://international-review.icrc.org/articles/how-harmful-information-on-social-media-impacts-people-affected-by-armed-conflict-926.

27 Hayes, "Migration," 191–193.

28 These two examples are also cited by Miriam Bradley, *The Politics and Everyday Practice of International Humanitarianism* (Oxford University Press, 2023), 410–411. For "transnational repression" mentioning 36 States, see Yana Gorokhovskaia and Isabel Linzer, *Defending Democracy in Exile: Policy Responses to Transnational Repression* (Freedom

had already formulated a specific request to States to respect the privacy and protection of its data and to refrain from using it "in any manner that would undermine the trust of the people" at the time of the breach.[29]

For 72% of the caseloads, the FLN mentioned specific mitigation measures in the record sheet. Individual notifications were mentioned as the principal mitigation measure, many of which were already planned, in progress, or completed at the stage of this additional risk assessment effort. Going beyond notifications, more community-based preventive measures were mentioned in the sheets, such as engaging other humanitarian actors working with affected populations and community leaders, distributing informative material for beneficiaries on risks related to data breaches, and holding sessions for beneficiaries and staff to be able to identify and mitigate risks. This included developing material to explain risks specifically to children. For the remaining 28% of caseloads, mitigation efforts were not deemed possible or necessary, for the same reasons as already outlined above: either because risks were ultimately considered so small and unlikely that the effort and resources needed to notify were considered disproportionate, or due to exposing beneficiaries to potential secondary harm through the act of notification. The latter consideration was particularly important, as this additional exercise explicitly included beneficiaries whose data was not breached in the first place, so there was no need to warn them.

This significant exercise to record, potentially re-do with the proposed particular methodology, and report risk assessments and mitigation actions was, on the one hand, remarkably well received by the FLN practitioners, as is evident from the high response rate. On the other hand, critical voices were also noted. Some members of the FLN found the exercise to be too abstract in its proposed methodology, disproportionate to the actual risks that the data breach posed, or took the view that something 'simpler' or more tailored to the reality of each National Society or ICRC Delegation could have sufficed, rather than a centralised exercise as was done.[30]

It was worth recalling that when the exercise was undertaken in the first half of 2022, no actual consequences of the data breach had been found, which also explains why the exercise remained theoretical and abstract. Concerns were also raised that the effort required for this exercise and the additional mitigation efforts may have worsened certain trade-offs. For example, the time and manpower invested in reflecting on caseloads, completing record sheets, and taking additional mitigation action could have been considered

House, 2022), https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf.

29 RCRC Movement, *Resolution Restoring Family Links*, Point 10/11.

30 ICRC, *Report on the Risk Assessments*, 5.

to have slightly delayed the resumption of normal service provision or other activities, due to the resources it tied up.

The question thus remains whether this exercise went far enough or went too far: should the FLN have recorded, reviewed, reported, compared, and learnt more about assessing risks and options to design mitigation action in more detail, maybe tailoring the methodology and reporting to each context, each caseload, and, ultimately, for each and every individual concerned? Or did the additional exercise create potentially unjustified workloads and draw excessive public attention to the data breach beyond what was ethically required?

Was the Additional Risk Exercise a Step Too Far? Is There a Need to go 'Backwards'?

The mixed reception of the additional exercise to record, potentially re-do, and report on risks amongst FLN practitioners shows that there is some complexity in doing justice to the data protection guidance in practice. Three aspects deserve closer attention: the question of what is disproportionate, who defines the level of risk that a data breach presents to individuals, and why the FLN cared so much about 'getting it right'. Reflecting on these suggests the importance of striking a balance, which can even include going "backwards" with certain ambitions, for example, with the aspiration to widely inform about a data breach.

With regard to the proportionality of the invested efforts, practitioners perceived a trade-off between investing in an (additional) exercise to record, potentially re-do, and report risk assessments and the resumption of services and other activities deemed of value to the beneficiaries. Ethically, this is not an unusual dilemma: 'moral choices' between 'two good things' are not straightforward to address. While the aim must always be to do both – in this context, to recommence the humanitarian services *and* mitigate any harmful effects of the data breach – in practice a balance must be struck.[31] Borrowing from the field of medical ethics, what counts may be the articulation of values and arguments and ensuring that care and attention are paid to considering and deliberating them. The ultimate question may not be whether it was the right decision (i.e. to notify or not; to further explore risks or to focus on services, to learn from a centralised reporting exercise) but, rather, whether the right procedure was followed, and appropriate time investment made, to make the decision in the first place.[32] Following a centrally set procedure and

31 On moral choices, see Slim, *Humanitarian Ethics*, 157–161.
32 Dunn and Hope, *Medical Ethics*, 83.

methodology can be a way to ensure that care and attention are duly paid by all concerned, and enable this to be recorded as such.

Another key concern raised was that it was too difficult to identify what the risks were that beneficiaries should be protected from, now that their data may have been breached. This issue relates to what has been called the "infinite vulnerability" of data, in the sense of "uncertain and as yet undetermined types of harm".[33] This was, as already mentioned, compounded in the case of the 2022 data breach by the lack of evidence of the consequences of the breach at the time of undertaking the additional risk assessments. In this situation, it was conceptually challenging to imagine and mitigate all kinds of potential scenarios, while avoiding construed and possibly alarmist outcomes. It was apparently equally challenging, if not impossible, to explain these often very theoretical and abstract risks to beneficiaries.

An underlying question is whether the FLN and its practitioners should have assumed the role of assessing risks to beneficiaries and data subjects on their own before deciding whether to notify due to secondary harm considerations, or whether this is not, in fact, the role of the affected persons themselves and that only they can consider harms, meaning there should always be a notification. The concept of 'relational risk' is relevant here: the necessity to acknowledge that the understanding of what has happened that presents a risk (the breach) is dependent on the perceived value of the object at risk (the data). Risk will vary for each person and situation, and can be considered culturally determined, variable, and continuously changing.[34] As such, this created another ethical dilemma or even a paradox: how can data subjects and beneficiaries be asked to assess their risks, if informing them of the risk, or simply approaching them to do so, can create more harm than the potential data breach itself?

A third and final type of criticism queries data protection and the guidance on dealing with data breaches more fundamentally, asking whether the underlying norms and values that data protection represents are truly global, universal, and acultural.[35] In one particular example, national authorities that were informed about the data breach suggested that data protection was a 'Western concept' that did not apply to the local context.[36] Cultural differences in underlying values such as privacy are considered to exist even between

33 Sandvik, *Humanitarian Extractivism*, 71.

34 Åsa Boholm and Hervé Corvellec, "A relational theory of risk," *Journal of Risk Research*, 14, no. 2, (2011), 175–190, http://dx.doi.org/10.1080/13669877.2010.515313.

35 For universal versus acultural values in the sector: Xabier Etxeberria, "The Ethical Framework of Humanitarian Action," *Reflections on Humanitarian Practice. Principles, Ethics and Contradictions*, edited by the Humanitarian Studies Unit (Pluto Press, 2001), 84–85.

36 ICRC, *Report on the Risk Assessments*, 5.

Western states.[37] If one, however, goes back to the *raison d'être* of data protection, to 'do no harm', assessing and mitigating potential risks of a data breach with care and attention is the ethically right action to take in general, even if the conclusion in certain contexts may, indeed, be that the data breach was not of great concern or interest to data subjects, beneficiaries, or authorities. Reflecting on this should be considered the ethically correct step regardless of potential variations in norms and values that underlie data protection rules.

The other element of this criticism was that both the general data protection guidance and the specific guidance provided by the ICRC for the additional risk assessment exercise focused on individual notifications as the main pillar of response, and did not sufficiently acknowledge community-based approaches to assess and mitigate risks. Medical ethics related to undertaking global research has also faced this allegation of an exaggerated focus on the individual and on individual consent, allegedly aligning more with the values of the humanitarian actor than with those of the communities concerned.[38] Once again, a balance must be struck, and the role of communities and community leaders to protect members from risks from data breaches should be acknowledged. In fact, such interaction with stakeholders and community members was mentioned in the report sheets for the additional risk exercise. For example, leaders of family associations (of missing persons) were consulted and informed about the data breach, even if these were, in fact, neither data subjects nor authorities.

A final question that was not specifically recorded as having been asked by FLN practitioners, but which may have been pondered, is what role considerations around accountability and retention of trust in the FLN played in the decision to introduce an additional reporting exercise. Humanitarian actors depend on trust, both of beneficiaries who entrust their data, and of donors who provide funding, trusting in the professionalism of humanitarians to handle the data safely and according to data protection standards.[39] This concern is also reflected in the FLN's Code, which states that communication on data breaches may not be required if "it would adversely affect a substantial public interest, including the viability of the data controller's operations".[40] Ethically, this may not be a real dilemma, in the sense that it seems valid for a humanitarian organisation to care that its services continue for the benefit of people needing them. The main consideration here is one of trade-offs, as already discussed above.

37 Uta Kohl, "The Right to be Forgotten in Data Protection Law and Two Western Cultures of Privacy," *ICLQ* 72 (2023): 738, 766, https://doi.org/10.1017/S0020589323000258.

38 Dunn and Hope, *Medical Ethics*, 109–117.

39 Sandvik, *Humanitarian Extractivism*, 89–90.

40 RCRC Family Links Network, *Code of Conduct*, Point 2.3.8.

Conclusions and Outlook

Returning to the initial question asked in this chapter: this was probably not a catastrophic event that fundamentally changed the way humanitarians think about data protection, at least insofar as no evidence of harmful misuse appears in the future. As described in this chapter, it was, rather, an occasion to demonstrate that the available guidance and codes of conduct, developed in the past decade by the ICRC in the context of restoring family links, were actionable and widely accepted. A response to the data breach that was 'by the book' was possible and was, in fact, adequately delivered. The decision of the ICRC to be transparent about the data breach thus appears not to have created a larger issue for the humanitarian sector; on the contrary, it indicates that this was the correct step to take. It should, however, be noted that the materialisation of potential threats following the data breach – harmful publication or usage of the data – might have been a catastrophic event in itself.

This chapter has highlighted the complexities of assessing and mitigating risks emanating from data breaches, not only for the individuals whose data was hacked but potentially also for other beneficiaries who entrusted their data to the FLN. On the one hand, going 'beyond the book' and embarking on an additional risk assessment exercise showed the relevance and validity of key concepts such as disproportionality and the need to consider secondary risks prior to proactive notifications. On the other, a review of this exercise revealed that responding to a data breach can, at times, raise fundamental questions and concerns of an ethical nature. As for humanitarian action in general, responding to a data breach requires "situational ethics", a need to be flexible rather than to take "preset criteria and apply them blindly", and to explore compromises and trade-offs when principles "bump into one another".[41] Most importantly, ethical action needs ethical thinking, reflection and deliberation, and a capacity to ask the right questions.[42] The current data protection guidance for handling data breaches provides a valid framework but, rather than understanding it as a technical exercise, it needs to be seen as a complex endeavour that will require ethical reflections. Ultimately, judgement calls on the right level of effort to be invested in risk assessment and mitigation will be required: going far enough, but not too far either.

In the end, the correct question to be asked may not be whether humanitarian actors are ready and capable of responsibly dealing with the consequences of data breaches – technically, practically, and ethically – but, rather, whether humanitarian actors can make their data less attractive for breaches in the first place. Rather than honing skills to respond to data breaches, calls have been

41 Thomas G. Weiss, *Humanitarian Business* (Polity, 2013), 177–179.

42 Slim, *Humanitarian Ethics*, 137; Reina C. Neufeldt, *Ethics for Peacebuilders: A Practical Guide* (Rowman and Littlefield, 2016), 3–11.

made for more awareness of the intrinsic and growing risks of the pursuit by humanitarian actors for ever more digitalisation and interconnected centralisation of data.[43] This may also imply going "backwards" in certain ambitions of the sector.

If holding the personal data of a particular individual could have serious consequences for this person, to the degree of being life-threatening and thus truly catastrophic if breached, the best solution may simply be for the FLN to refrain from collecting this data in the first place. This, of course, implies withholding the humanitarian service to find one's family, or be found by them, that this person may desire above all else, which again raises questions of an ethical nature that are abundant in humanitarian action, including as regards data protection practices.

43 Sandvik, *Humanitarian Extractivism*, 91–92; David Forsythe, *The Contemporary International Committee of the Red Cross* (Cambridge University Press, 2024), 361, https://doi.org/10.1017/9781009387002.

14

GROWING DATA PROTECTION MATURITY IN HUMANITARIAN ACTION

Changes in the Understanding of Key Concepts

Dogu Han Buyukyagcioglu[1]

Introduction

Over the last decade, data protection in humanitarian action has matured towards a more robust framework of a set of principles and concepts that are reshaped in practice, including the notion of confidentiality, the understanding of consent, and the principle of accountability. It is possible to characterise this movement as progressive, perhaps not steady or linear, but certainly dynamic, mainly shaped by the interplay between the normative and practical developments experienced by two fields: approaches in humanitarian action and data protection.

Processing of personal data is necessary for humanitarian action, which means, if we look at relevant General Assembly resolutions for a definition, saving lives and alleviating suffering while upholding and restoring the personal dignity of individuals affected by natural disasters or armed conflicts.[2] This necessity has created an inevitable interplay over the past decade where humanitarian principles have informed and influenced data protection principles, and *vice versa*.

1 The opinions and views expressed in this chapter are the author's own and do not necessarily represent those of the United Nations High Commissioner for Refugees (UNHCR).

2 UN General Assembly, *Strengthening of the coordination of humanitarian emergency assistance of the United Nations*, Resolution 46/182 adopted on 19 December 1991, https://docs.un.org/en/A/res/46/182.

DOI: 10.4324/9781003650164-20

Modern data protection and privacy legislative frameworks have witnessed "an evolution and not a revolution"[3] marked by the fine-tuning of the application of a set of rules in particular contexts and the establishment of higher standards; but also, in parallel, a move towards the development of standards that are globally applicable and implementable, such as those set out in Convention 108.[4]

In the meantime, humanitarians have established their own data protection and privacy frameworks which are relevant and implementable in their own context. In this chapter, the terms "humanitarians" or "humanitarian actors" refer to international organisations (IOs) and United Nations (UN) entities with defined mandates for humanitarian action that are set out under public international law. Such humanitarian actors share three common characteristics: they are authorised or otherwise tasked by the international community to perform certain humanitarian functions and activities; their mandates or statutes include adherence to humanitarian principles at the highest level; and they enjoy certain privileges and immunities that render the application of national and regional legislative frameworks unenforceable against them so IOs and UN entities can perform their mandates independently.[5] Therefore, they establish their own normative frameworks. These three common characteristics make humanitarian actors relevant and suitable subjects for analysis for the arguments presented in this chapter.

The International Committee of the Red Cross' (ICRC) Rules on Personal Data Protection and the United Nations High Commissioner for Refugees' (UNHCR) Policy on the Protection of Personal Data of Persons of Concern to UNHCR were the first comprehensive frameworks of their kind in the humanitarian sector, establishing a mandatory set of principles for data protection within their respective organisations. Such efforts were followed by a high-level commitment by the humanitarian community when the UN High-Level Committee on Management formally adopted the Principles on Personal Data Protection and Privacy on 11 October 2018.

The growing data protection maturity of humanitarian organisations has been just as important as, if not more important than, the adoption of comprehensive and mandatory frameworks in this field by humanitarians.

3 Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means," *Information & Communications Technology Law* 28, no. 1, (2019): 65–98, https://doi.org/10.1080/13600834.2019.1573501.

4 Alessandro Mantelero, "The future of data protection: Gold standard vs. global standard," *Computer Law and Security Review* 40, (2021), https://doi.org/10.1016/j.clsr.2020.105500.

5 Massimo Marelli, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders," *Computer Law & Security Review* 50, (2023), https://doi.org/10.1016/j.clsr.2023.105849.

Whether this maturity has reached a successful or acceptable level is debatable, but it has determined the degree to which humanitarian organisations have absorbed these global standards in data protection and privacy, and particularly how they have been adopted within their internal normative frameworks and put into practice.

Over the last ten years, the level of data protection maturity within humanitarian organisations has defined both the manner and the extent to which the evolving global standards in data protection have been integrated into humanitarian action. As this maturity advanced, it allowed for more interaction and mutual influence in this multidimensional relationship, collectively driving the development and institutionalisation of data protection and privacy norms in the humanitarian sector. As it grew and enabled more interaction, humanitarians' engagement with external data protection frameworks evolved beyond passive adoption of their principles and standards. Instead of merely implementing standards, which sometimes did not fully fit the context, humanitarians started to rethink, reinterpret, and refine key concepts, standards, and practices, ensuring that data protection remains relevant to the challenges of humanitarian action.

Humanitarian actors, in their own context, were familiar with the concepts and principles that were introduced by the emerging and growing data protection and privacy frameworks. However, in parallel and in addition, humanitarian actors had their own set of principles which defined the nature, objective, and scope of their interventions. This unique perspective, coupled with the realities of the operational contexts in which humanitarian actors functioned, contributed to reshaping data protection principles and key concepts in practice.

In order to respond to the last ten years' humanitarian crises of unprecedented nature and scale, humanitarian actors have had to leverage technology despite its inherent risks.[6] At a minimum, humanitarians now depend on technical digital infrastructure such as cloud-hosting services, the Microsoft 365 suite, or similar tools for coordination, and communication apps to manage day-to-day operations. The use of these tools is fundamental to basic coordination, data storage, and data sharing among humanitarians.

Beyond such inevitable digital infrastructure, humanitarians are faced with a strategic decision to resort to more innovation-oriented solutions, for instance, predictive analytics, digital registration platforms, and other advanced digital tools that depend on partnering with the tech industry. This is due to the scale of crises where leveraging technology has value for analysis

6 Ana Beduschi, "Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks," *International Review of the Red Cross* 104, no. 919 (2022), https://doi.org/10.1017/S1816383122000261.

and decision-making relating to the provision of lifesaving assistance and protection interventions, or for effective and evidence-based programming and design of these interventions.

It is worth noting that, for many humanitarian actors, adopting more sophisticated digital tools is not simply a matter of cost reduction. Consider, for instance, a reception centre that receives 5,000 new arrivals each day.[7] Introducing self-service kiosks[8] or a fully digital registration system is not done solely to save money; it alleviates long queues and reduces the physical and emotional burden on vulnerable individuals, such as the elderly, those with serious medical conditions, lactating mothers, or the sole wage-earner in a refugee family, whose daily earnings evaporate if they must wait for hours. Similarly, a digital service capability can protect undocumented asylum seekers from inadvertently coming into conflict with the local authorities on their way to receive assistance or documentation. In each case, the decision to embrace the innovation-oriented technology does not stem from a simple desire to modernise, or a determination by the big-tech companies, but from a strategic imperative to optimise lifesaving assistance, protect vulnerable populations, and design more evidence-based programmes that alleviate human suffering.

Notwithstanding this, the distinction between what is essential and what is part of a strategic direction is shrinking. Once humanitarians invite non-humanitarian tech vendors to provide essential digital infrastructure, they also invite the associated risks, which can be as significant as those posed by innovative initiatives.

As a result, the sector has reached a point where humanitarians are collecting more personal data than ever, often alongside private and public sector entities with competing interests that are not necessarily guided by humanitarian principles. This brings into play the need for rethinking the principle of accountability from both a data protection and humanitarian perspective.

This chapter presents a critical interrogation of key concepts in data protection and privacy, such as confidentiality, consent, and accountability from a humanitarian viewpoint. Over the past decade, a semantic cross-pollination has occurred between data protection practitioners and humanitarians, which is seen in the mutual influence and exchange of terminology, concepts, and meanings between the two distinct fields, resulting in a rich understanding and practice in both of them. This has resulted in a change of understanding of key concepts in theory and in practice.

7 UNHCR Registration Centre in Amman, Jordan. UNHCR, "New registration site in Jordan clears Syrian refugee backlog," 2 September 2013, https://www.unrefugees.org/news/new-registration-site-in-jordan-clears-syrian-refugee-backlog/.

8 UNHCR, "Jordan Operational Update," 2025, https://data.unhcr.org/en/documents/details/115786.

By rethinking such key concepts, this chapter represents an invitation to both humanitarians and data protection specialists to deepen their collaboration and further this conversation through intellectual and practical engagement.

From Confidentiality to Data Protection

Early attempts at putting in place a set of rules around how humanitarian organisations should process personal data put confidentiality at the centre. For instance, it is no coincidence that the initial personal data normative frameworks, which predated the 2015 Policy on the Protection of Personal Data of Persons of Concern to UNHCR, were either called "Confidentiality Guidelines" or had a strong emphasis on confidentiality.[9]

Such normative frameworks were naturally were scoped like a quasi-classification and disclosure guidance, whereby confidentiality was the rule and disclosure, which required the consent of the affected individual, was the exception. A similar understanding and scoping in the early examples of data protection guidance in humanitarian organisations can be found under other guidance material of organisations such as the World Food Programme (WFP)[10] or the International Organization for Migration (IOM).[11]

The strong emphasis on confidentiality is both appropriate and necessary in humanitarian contexts. Unauthorised or accidental disclosure of personal data by humanitarian actors may have severe consequences for affected people, which, depending on the context, may range from discrimination to *refoulement*,[12] or targeted killings. Similar risks, varying in nature and severity, also exist for humanitarian workers.

9 Although we can trace efforts for a data protection framework and a draft policy on data protection for UNHCR back to the 1980s, the first related UNHCR guidance on the subject matter had a confidentiality focus. See, for instance, UNHCR, "Confidentiality of information concerning individual refugees or asylum seekers in discussions with countries of origin," *IOM/12/90 – FOM/12/90*, 12 February 1990; UNHCR, "Confidentiality Guidelines"; *IOM 71/2001- FOM/68/2001*, 24 August 2001. For a detailed analysis of UN Guidelines for the Regulation of Computerized Personal Data Files, see Chapter 7, David Erdos, "Data Protection Regulation and International Humanitarian Organisations: Revisiting the Origins and Importance of the UN Guidelines on Personal Data Regulation (1990)".

10 WFP, *Guide to Personal Data Protection and Privacy*, 2016, https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

11 IOM. *IOM Data Protection Principles.* Geneva, 2009, https://www.iom.int/sites/g/files/tmzbdl2616/files/documents/2023-08/iom-dp-principles-en.pdf.

12 Expulsion or return of a person (*refouler*), in any manner whatsoever, to territories where their life or freedom would be threatened, on account of their race, religion, nationality, membership of a particular social group or political opinion, or where there are substantial grounds for believing that they would be in danger of being subjected to serious human rights violations, notably torture or other forms of cruel, inhuman or degrading treatment

In fact, confidentiality was never presented in isolation and has always been part of a broader set of standards that govern humanitarian action, including informing individuals about interventions and seeking their opinions. The notion of confidentiality has long been integral to humanitarian professional standards and a core principle of codes of conduct for humanitarian actors.[13]

For humanitarians, confidentiality was more than a classification level or a standard that seeks protection against unlawful or unauthorised disclosure. It is an integral part and parcel of the design of humanitarian and protection interventions. Such standards do not only apply to personal data, whether processed in digital or paper format, but also to the very design of processes for humanitarian interventions. For instance, a typical reception centre of a humanitarian organisation is designed in a way that can provide humanitarian services to individuals while upholding confidentiality. Such design considerations include structural arrangements, e.g. the selection of the registration site, its layout including the distance between waiting areas, registration desks, protection desks, litigation desks, and dedicated areas that provide additional confidentiality, as well as further measures such as rigging up curtains or screens and cordoning off certain areas.[14]

Confidentiality is not only important for safeguarding the safety and dignity of affected populations in a broad sense, but it is an equally important element for building rapport with the individuals humanitarians are aiming to assist and protect during protection interventions or when conducting vulnerability assessments. Therefore, the humanitarian understanding of confidentiality is about protecting affected people.

Having said that, the initial normative frameworks for data protection and privacy of humanitarians placed an overemphasis on confidentiality and paid insufficient attention to how processing of personal data by humanitarian actors should be limited after it has been collected, or regarding how data subjects can maintain agency over their own personal data. Such an approach naturally resulted in data governance having a limited scope linked to non-disclosure and shifted the focus of humanitarians away from where it should have been. Instead of focusing on limiting the impacts of personal data processing on affected people through a rights-based approach, humanitarians focused on ways to limit its disclosure. As a result, data protection became

---

or punishment, or arbitrary deprivation of life. UNHCR, "Access to territory and non-refoulement", *Emergency Handbook*, 2025, https://emergency.unhcr.org/protection/legal-framework/access-territory-and-non-refoulement.

13 UNHCR, *Code of Conduct*, 2004.

14 For the recommended layout of a typical reception centre, UNHCR, *Guidance on Registration and Identity Management*, 2018, https://www.unhcr.org/registration-guidance/.

more about protecting the data instead of protecting the individuals who are behind the data.

One clear indication of this understanding was that data protection practitioners in humanitarian entities were only being consulted when the organisations were negotiating data sharing agreements, and not sufficiently consulted in the design of the humanitarian interventions. Their inputs were often perceived as "the cost of doing business" or bureaucratic compliance efforts.

Over the past decade, considerations around the collection, use, and sharing of personal data have expanded beyond confidentiality, leading humanitarian actors to develop more comprehensive data protection frameworks. These efforts to establish normative standards for data protection and privacy, examples of which were discussed earlier in this chapter, reflected the "spirit of the times" and evolving national and regional data protection legislation in parallel. Moreover, the process was also impacted by the inevitable interaction between humanitarian actors and private sector entities or non-governmental organisations (NGOs) that are subject to such national and regional legislation. For instance, such interaction required contractual arrangements to be put in place to govern data flows, which resulted in humanitarians and other entities subject to national legislation starting to start using a similar terminology to define roles, responsibilities, principles, and standards.

Advances in technology and the broader shift toward digital transformation have narrowed the practical scope of confidentiality, as humanitarians increasingly rely on private vendors and infrastructure providers who do not share humanitarian objectives and pursue very different interests. This dependence introduces new risks and calls for an approach that goes beyond an understanding of confidentiality as limits of disclosure and one that supports a rights-based approach through requiring minimum standards and implementing coherent transfer mechanisms.[15]

Against this background, there remains room for improvement with respect to the adoption of an expanded understanding of data protection beyond confidentiality. Future normative frameworks must refrain from putting their central focus on non-disclosure and aim to mainstream data protection principles at all stages of processing, particularly in the collection and further processing of personal data.

Confidentiality needs to be redefined in a way that puts the individuals behind the data first, rather than focusing on protecting the data itself. The latter carries the risk of presenting siloed and duplicated efforts among humanitarian actors, where data protection is often put forward as an impediment to a concerted response.

15 See Chapter 5, "Digital Transformation and the Humanitarian-Development Transition: The Role of Digital Public Infrastructure and Data Protection".

Humanitarians must aim to establish normative frameworks that include coherent legal transfer mechanisms to facilitate the data flows necessary for coordination in a principled and efficient way, consistent standards that are anchored in humanitarian principles with accountability, and redress mechanisms that ensure protection follows the personal data when transferred among humanitarian organisations.

Are We Referring to the Same Concept of Consent?

Consent is another key concept that is widely used by humanitarians and data protection practitioners.

Informed consent has always been an indispensable part of the professional and ethical standards[16] followed by humanitarians in their line of work, with the aim of giving control to individuals in relation to the assistance programmes and other interventions performed in the context of a humanitarian or protection response. Humanitarians are used to informing affected individuals and ensuring their understanding of the processes and procedures they will go through, including using modern techniques such as cognitive interviewing.[17]

When data protection and privacy frameworks introduced consent as a legal basis for processing personal data, humanitarians incorporated it into their data protection guidance or principles as is, and initially without much questioning.[18]

Modern data protection frameworks conceptualise consent as an "enabler" for processing sensitive or special categories of personal data, or for international transfers, both of which are very relevant and often necessary in humanitarian action. This is another reason why humanitarians need to have a systematic and consistent approach towards consent.

While reliance on consent is rational and applicable in the context of other sectors, for humanitarians, the conditions in which the consent of the individual is sought, as well as the power dynamics involved, render it very hard to obtain consent that is free, informed, specific, and clear.

16 ICRC, *Professional Standards for Protection Work by Humanitarian and Human Rights Actors During Armed Conflict and Other Violence*, 4th Edition, 2024.

17 This is an integral part of the "PEACE Model of Interviewing" adopted by UNHCR for protection interviews. See UNHCR, *Procedural Standards for Refugee Status Determination Under UNHCR's Mandate*, 26 August 2020, https://www.refworld.org/policy/legalguidance/unhcr/2020/en/123306.

18 For instance, informed consent sits at the centre of IOM data protection principles. *IOM Data Protection Principles*, 2009, https://www.iom.int/sites/g/files/tmzbdl2616/files/documents/2023-08/iom-dp-principles-en.pdf.

But at the same time, informed consent is a concept that is central to humanitarians. From an ethical perspective, it is important to place affected populations at the centre of humanitarian interventions and grant them agency and control. This has resulted in semantic cross-pollination between humanitarian action and data protection, which has naturally caused an amalgamation of existing processes for obtaining informed consent in humanitarian action, and using such consent as a legal basis for processing personal data.

The result is a risk of overemphasis on consent by humanitarians resembling the outdated models of normative frameworks resting upon an overestimation of the individual dimension and consent.[19] Such emphasis ignores the dilemma of using consent as a legal basis for personal data processing in humanitarian action and the original aim of obtaining informed consent as part of professional standards for protection work.

It is important to recognise that consent as a legal basis for processing personal data differs fundamentally from informed consent that is required by specific ethical[20] or professional standards or frameworks. This distinction was clearly articulated by the European Data Protection Board in 2019, in relation to the use of informed consent in clinical trials.[21] Similarly, in the humanitarian context, the interchangeable use of consent as a legal basis and informed consent promotes confusion and compromises the principle of fair and transparent processing.

There have been ample academic and non-academic discussions in law, medicine, and other relevant disciplines on the shortcomings of consent.[22] This chapter will not repeat those but will acknowledge that it did not take

19 Mantelero, *"The future of data protection: gold standard vs. global standard"*.

20 Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. Text with EEA relevance, http://data.europa.eu/eli/reg/2014/536/oj.

21 "Provisions of Chapter V CTR on informed consent, in particular Article 28, respond primarily to core *ethical requirements* of research projects involving humans deriving from the Helsinki Declaration. The obligation to obtain the informed consent of participants in a clinical trial is primarily a measure to ensure the protection of the right to human dignity and the right to integrity of individuals under Article 1 and 3 of the Charter of Fundamental Rights of the EU; it is not conceived as an instrument for data protection compliance," EDPB, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (art. 70.1.b)*, 23 January 2019, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf [emphasis added].

22 Benjamin Thomson, S. Mehta, and C. Robinson, "Scoping review and thematic analysis of informed consent in humanitarian emergencies," *BMC Med Ethics* 25, no. 135 (2024), https://doi.org/10.1186/s12910-024-01125-w; Lydia A. Bazzano, Jaquail Durant, and Paula Rhode Brantley, "A Modern History of Informed Consent and the Role of Key Information," *Ochsner Journal* 21, no. 1 (2021), https://doi.org/10.31486/toj.19.0105.

long before humanitarians started to join the discussions around the challenges of obtaining valid consent[23] in a humanitarian response.

The growing maturity of data protection in humanitarian action calls for revisiting humanitarians' understanding of consent when it comes to personal data processing. Consent, when considered as a legal basis for processing personal data for humanitarian interventions, is not free, because individuals cannot withhold or withdraw it without potential detrimental impacts. It is often not specific and not very well informed.

Transparency, whether you consider it as a standalone principle[24] or a part of the principle of fair processing, requires informing data subjects accurately regarding the processing of their personal data. A fundamental problem with relying on consent in humanitarian action is that it gives data subjects the impression that the personal data processing is based on their consent, whereas the foundational elements of consent do not exist, mainly because of a power imbalance. Technological developments and the trend of digital transformation tend to reinforce, and not reduce, these negative power dynamics.

And by using informed consent as a legal basis for personal data processing in a context where there is great power imbalance between the parties, humanitarians risk going against the very objective that they aim to uphold by obtaining informed consent. It not only creates a false sense of agency and control for individuals, it also abrogates the responsibility of the humanitarian actors as data controllers[25] and puts the burden on affected peoples' choices, which are often made in life-or-death situations.

On the contrary, accountability should be brought back to where it belongs. It is the humanitarian actors' responsibility to assess the potential risks of a particular personal data processing operation in a humanitarian intervention and mitigate such risks. Humanitarians should find alternative methods of empowering individuals to make informed decisions about how their personal data is processed in the context of a humanitarian response, including why such interventions exist and why such means and methods are employed, and their rights as data subjects that allow individuals to make informed decisions about their personal data, including to opt out from processes. This approach, which makes humanitarians accountable, is not driven from a paternalistic perspective that presumes affected populations cannot decide; but, as Devidal

23 Massimo Marelli, "Data Protection Principles in Humanitarian Action," *Handbook on Data Protection in Humanitarian Action*, Marelli ed. (Cambridge, 2024), https://doi.org/10.1017/9781009414630.

24 UNHCR, *General Policy on Personal Data Protection and Privacy*, 20 December 2022, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207.

25 Fred H. Cate and Viktor Mayer-Schönberger, "Notice and Consent in a World of Big Data," *International Data Privacy Law* 3, no. 2 (2013), https://doi.org/10.1093/idpl/ipt005.

argues, it is because humanitarians have the duty to do so in order to respect and protect affected populations' safety, dignity, and autonomy.[26]

Moving away from consent in data protection in humanitarian action should not necessarily result in ceasing to obtain consent in a humanitarian response; but it should make a clear distinction, as the principle of transparency would require, between what constitutes a legal basis and what is an ethical or professional requirement.

Technological developments would certainly help, but the assumption of accountability by humanitarians does not necessarily require reliance on advanced technology. It requires processes for conveying clear information in a language and manner that is understandable, intake mechanisms to hear, assess, and take into consideration objections, and an implementable and fair redress mechanism to hear grievances.

Rethinking Organisational Accountability

The growing maturity in data protection in humanitarian action has also impacted the understanding of the concept of accountability and presented an opportunity for further engagement between humanitarians and data protection practitioners.

For humanitarians, accountability has been a commitment to affected people to uphold the principle of humanity. Accountability to affected people has been a promise since the early 1990s,[27] and aims to inform the design of humanitarian interventions for transparency, fairness, and participation by affected individuals. It continues to be a relevant and central commitment.[28]

And for data protection practitioners this is a key data protection principle. It aims to clarify and make visible to data subjects who are responsible for the processing of their personal data.

While there is room for growth in maturity for accountability when it comes to data protection in humanitarian action, this common conceptual approach between data protection practitioners and humanitarians is certainly promising ground for further engagement. Existing safeguards and processes foreseen under the commitment of accountability to affected people can

26 Pierrick Devidal, "Lost in digital translation? The humanitarian principles in the digital age," *International Review of the Red Cross* 106, no. 925 (2024), https://doi.org/10.1017/S1816383124000080.

27 UN High Commissioner for Refugees (UNHCR), *A Framework for People-Oriented Planning in Refugee Situations Taking Account of Women, Men and Children*, 1992, https://www.refworld.org/policy/opguidance/unhcr/1992/en/75968.

28 UNHCR, *Strategic Directions 2022–2026*, 1 March 2022, UNHCR Strategic Directions 2022–2026 | Global Focus, https://www.unhcr.org/media/unhcr-strategic-directions-2022-2026.

be utilised to realise data protection and privacy principles in humanitarian responses in a meaningful and implementable way. And humanitarians can draw lessons from how the principle of accountability in data protection is upheld through a set of requirements, standards, and redress mechanisms.

The normative frameworks that humanitarians have produced in the last decade have increasingly put an emphasis on internal and external accountability structures.[29] Now it is time to further implement these structures, so that they do not remain as mere organigrams and procedural rules distinguishing roles, accountabilities, and authorities.

The principle of accountability in data protection in humanitarian action is particularly important because of what is at stake – that is efforts to save lives and alleviate human suffering. It becomes even more important as such efforts are made by humanitarians inevitably engage with other actors with distinct and often competing interests. There is a need to acknowledge such competing interests in emergency/humanitarian settings and establish a notion of internal and external accountability for humanitarians.

Internal and external accountability requires looking into a broader list of applicable legal/legitimate bases, and a clearer framework for proportionality and balancing tests, ensuring that personal data processing is necessary, justified, and, overall, in line with the humanitarian principles. The last point is important. In order to stay true to their humanitarian character, humanitarians will need stronger anchors to their own principles in addition to the data protection and privacy principles.

Modern data protection and privacy frameworks offer a set of legal bases that are relevant for humanitarian action, such as vital interest, public interest, and the legitimate interest of the controller. Such legal bases also come with requirements and standards which have the potential to be adopted and adapted into humanitarian work to achieve the principle of accountability.

Humanitarians must seek to develop comprehensive frameworks that give more room to these legal bases, and that elaborate on the conditions and parameters in which they can be used. The competing interests in a humanitarian setting require each of these legal bases, including the important grounds of public interest, to be subject to a balancing test when relied upon. Humanitarians have their own unique humanitarian principles and commitments that are helpful in contextualising parameters for such proportionality and balancing tests.

29 See, for instance, the Personal Data Protection Review Committee under UNHCR's framework. UNHCR, *General Policy on Personal Data Protection and Privacy*, 20 December 2022, or the Data Protection Commission established under the ICRC framework, "ICRC Rules on Personal Data Protection" (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

To uphold the commitment of accountability to the affected populations, humanitarians must put in place procedural safeguards establishing two layers of controls: one that includes measures and approaches that are *ex ante*, and others that are *ex post*.

The *ex ante* measures include the humanitarian organisations, as data controllers, performing a balancing test prior to commencing the personal data processing to demonstrate that the processing is legal. Such a test must define the "legality" of the processing and look at competing interests in a humanitarian setting, while aiming to put the interests of the affected populations at the centre by anchoring to humanitarian principles.

Ex ante measures must also include a thorough due diligence process performed before starting any data-processing activity or engaging with an external stakeholder. From a humanitarian standpoint, this process must extend beyond mere data protection compliance, identifying high-risk processing operations to trigger a Data Protection Impact Assessment (DPIA) or conducting a transfer-risk assessment. It must also apply a protection lens, examining who those external stakeholders are and whose interests they serve, for instance through human rights due diligence or detailed protection analysis as the context requires. In practice, this means that due diligence, particularly when partnering with technology companies or similar entities, must be both broader in scope and deeper in analysis.

The *ex post* measures include putting in place mechanisms and procedures allowing data subjects to object to processing of their personal data at any stage of the processing which brings their particular situation to the attention of the data controller. This should act as a litmus test that continuously checks and reconfirms the legality and proportionality of the personal data processing, and, if coupled with efficient and implementable intake and complaint mechanisms, should aim to implement meaningful and effective redress to achieve accountability.

The *ex post* measures also include acknowledgment of incidents or breaches relating to personal data processing when they occur,[30] and putting in place a series of actions to mitigate the negative impacts on affected populations.

Conclusion

Data protection and privacy considerations in humanitarian action should support the overall objective of humanitarian interventions – that is to save lives and alleviate suffering while upholding and restoring the personal dignity of

30 See Chapter 12, "By the Book, Beyond and Backwards? Ethical considerations on the 2022 data breach affecting the Family Links Network of the Red Cross and Red Crescent Movement".

individuals affected by natural disasters, armed conflicts, and other situations of violence. Any analysis or measure that disregards such interconnections risks being impractical or even causing harm to the affected people humanitarians aim to serve.

The engagement between humanitarians and data protection specialists over the last decade has initiated a semantic cross-pollination, prompting a rethinking, reframing, and redefining of concepts such as confidentiality, consent, and accountability.

Yet there is still room for improvement. There are still too many humanitarian practitioners who do not feel concerned about data protection issues, while the real and full potential contribution of data protection specialists to the humanitarian sector remains underdone.

The maturity of data protection in humanitarian action is advancing. But its pace and scale will depend on the level and nature of engagement between the two disciplines.

15

DATA SHARING BETWEEN HUMANITARIAN ORGANISATIONS AND DONORS

Accountability, Transparency, and Data Protection in Principled Humanitarian Action

*Larissa Fast, Stuart Campo, and Gilles Cerutti**

Introduction

Humanitarian action has long been based on the collection of timely and reliable information on people in need. From household-level needs assessment survey results to details about delivering assistance to specific individuals, demographic groups or locations, disaggregated data from humanitarian contexts can provide valuable insights. The rising availability of and demand for such data in recent years has increased the incentives for humanitarian organisations to collect and share it, generally linking it to the improved coordination, accountability, transparency, efficiency and, critically, resourcing of their operations.

Donors play a key role in this dynamic, both as users and consumers of data and as drivers of its increased collection and analysis. Donors regularly request data from the organisations they fund in order to fulfil their own obligations and objectives.[1] Data sharing requests may serve multiple purposes: to check if intended objectives were reached, to account for the responsible use of public funds, to enrich the donor's understanding of different crises or contexts, to

* Mr Cerutti is expressing a personal point of view here. The opinions stated in this text should not be regarded as the official position of Switzerland or of the Swiss Federal Department of Foreign Affairs (FDFA).

1 In this article, we do not address data sharing between humanitarians or donors and host States, nor do we focus in detail on sharing between donors and "third-party monitors" (i.e. external bodies contracted to monitor and evaluate programmes) or donors and their constituencies.

DOI: 10.4324/9781003650164-21

support public communication efforts, and to justify and advocate for funding programmes, organisations, or crisis operations.

The collection and sharing of personal data raise challenging questions related to balancing accountability, transparency, and data protection in principled humanitarian action. One example relates to requests for the personal data of beneficiaries for the purposes of screening against counterterrorism and sanctions lists. Although humanitarian organisations are required to comply with counterterrorism measures and sanctions,[2] many argue that screening aid recipients – including by sharing their personal data – violates the humanitarian principles of humanity, impartiality, neutrality, and independence. In fact, many organisations have drawn a red line under such beneficiary screening, citing data protection regulations and humanitarian principles as the basis for denying donors' requests for personal data.[3] However, as we explore in this chapter, not all humanitarian organisations have the power and trusted position required to effectively push back on such requests.

In addition to requests for personal data, donors regularly ask humanitarian organisations to share potentially sensitive non-personal data. For instance, sharing seemingly innocuous data such as aggregated survey results can place already vulnerable people and communities at greater risk. What may be considered non-personal data can still allow for the re-identification of individuals, communities, and demographic groups. Re-identification occurs when data can be traced back or linked to an individual or group(s) of individuals because it is not adequately anonymised. For example, even if a humanitarian organisation removes direct identifiers such as a person's name or phone number from a data set, combining key variables such as location, language, or ethnicity can still allow for re-identification.[4] This can result in a violation of data protection, privacy, and other human rights and can allow for the targeting of individuals or groups with violence or other forms of harm.

Donors and humanitarian actors now widely recognise and strive to mitigate the risks associated with collecting and sharing personal and otherwise sensitive data. Whereas these risks were rarely discussed at the outset of the

2 Emanuela-Chiara Gillard, Sangeeta Goswami, and Fulco van Deventer, "Screening of Final Beneficiaries – a Red Line in Humanitarian Operations. An Emerging Concern in Development Work," *International Review of the Red Cross* 103, no. 916–917 (2021): 517–537, http://dx.doi.org/10.1017/S1816383121000448.

3 Kristina Roepstorff, Charlotte Faltas, and Sonja Hövelman, "Counterterrorism Measures and Sanction Regimes: Shrinking Space for Humanitarian Aid Organisations," *Centre for Humanitarian Action*, Berlin. (2020), https://www.chaberlin.org/en/publications/counterterrorism-measures-and-sanction-regimes-shrinking-space-for-humanitarian-aid-organisations/.

4 United Nations Office for the Coordination of Humanitarian Affairs, *Guidance Note: Statistical Disclosure Control* (Centre for Humanitarian Data, 2019), https://centre.humdata.org/wp-content/uploads/2019/07/guidance_note_sdc.pdf.

drive to adopt and deploy information and communication technologies in humanitarian action a decade ago,[5] they now dominate discourse in the sector around the increased use of data and technology to deliver aid, with data protection as a common foundational lens for actors across the system. However, despite progress in advancing data protection in humanitarian action over the past decade, the sector has yet to establish a common approach for balancing risks and benefits in practice vis-a-vis the data sharing relationship between humanitarian organisations and donors.

In September 2020, the Government of Switzerland, the International Committee of the Red Cross (ICRC), and the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data initiated a dialogue process to address this gap under the umbrella of the Humanitarian Data and Trust Initiative (HDTI).[6] The dialogue process involved two high-level meetings convened through Wilton Park,[7] two pieces of independent research to better understand potential risks[8] and existing practice,[9] as well as a series of stakeholder consultations that ultimately yielded the Principled Framework for Responsible Data Sharing Between Humanitarian Organisations and Donors.[10]

5 Gus Hosein and Carly Nyst, "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries," *Privacy International*, London. (2013), https://privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf.

6 The HDTI was convened by the UN OCHA Centre for Humanitarian Data, the Swiss Federal Department of Foreign Affairs, and the ICRC.

7 'Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Principled Humanitarian Action (WP1777),' Wilton Park, accessed 3 May 2025, https://www.wiltonpark.org.uk/event/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action-wp1777/; 'Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Principled Humanitarian Action – Towards a Common Approach (WP1777v2),' Wilton Park, accessed 3 May 2025, https://www.wiltonpark.org.uk/event/responsible-data-sharing-with-donors-accountability-transparency-and-data-protection-in-principled-humanitarian-action-towards-a-common-approach/.

8 Florian Westphal and Claudia Meier, "Research on the Specific Risks of Constraints Associated with Data Sharing with Donors for Reporting Purposes in Humanitarian Operations," Global Public Policy Institute, 2020, https://gppi.net/2021/09/06/data-sharing-with-humanitarian-donors.

9 Larissa Fast, "Data Sharing Between Humanitarian Organisations and Donors: Toward Understanding and Articulating Responsible Practice," *NCHS Paper* 06 (Norwegian Centre for Humanitarian Studies, 2022), https://www.humanitarianstudies.no/resource/data-sharing-between-humanitarian-organisations-and-donors/.

10 "A Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors", HDTI, accessed 3 May 2025, https://centre.humdata.org/a-principled-framework-for-responsible-data-sharing-between-humanitarian-organizations-and-donors/.

This chapter explores the key findings from the dialogue process and related efforts to improve data protection in data sharing. It describes the formal and informal dynamics and risks that characterise data sharing between humanitarians and donors, exposes persistent complications and challenges of data protection in the practice of data sharing, examines the prospects and pitfalls of a potential framework for data sharing between humanitarians and donors, and offers recommendations on navigating these issues collectively in the future.

From Institutional Policy and Practice to Frameworks for Collective Action

Humanitarian organisations have invested significantly in advancing data protection policies and practice over the past ten years. More robust data protection policies and guidance have created space for better practice, which in turn has driven more widespread awareness, buy-in, and uptake of policies and guidance in the sector. Whereas the establishment of a data protection policy appeared novel when the ICRC first adopted its Rules for Personal Data Protection in 2015,[11] having such a policy in place and actively investing in its implementation is now standard for organisations across the sector. As Dogu Han Buyukyagcioglu argues in this volume,[12] the "growing data protection maturity of humanitarian organisations has been just as important as, if not more important than, the adoption of comprehensive and mandatory frameworks".

To complement individual institutional investments, humanitarians have leveraged the maturity of data protection as a lens of analysis in the sector to develop frameworks for collective action and collaboration. This includes the ICRC Handbook on Data Protection in Humanitarian Action[13] and the Inter-Agency Standing Committee (IASC) Operational Guidance on Data Responsibility,[14] amongst others. While these frameworks provide common

11 ICRC, "ICRC Rules on Personal Data Protection" (2015, as updated April 2025), https://shop.icrc.org/icrc-rules-on-personal-data-protection-pdf-en.html.

12 See Chapter 14, Dogu Han Buyukyagcioglu, "Growing data protection maturity in humanitarian action: changes in understanding of key concepts in theory and in practice".

13 Massimo Marelli ed., ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition (Cambridge, 2024), https://doi.org/10.1017/9781009414630.

14 IASC, *Operational Guidance on Data Responsibility in Humanitarian Action*, (2023), https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action. N.B.: Data responsibility in humanitarian action is the safe, ethical, and effective management of personal and non-personal data for operational response, in accordance with established frameworks for personal data protection. While data responsibility is linked to data protection and data security, these terms are different. 'Data protection' refers to the systematic application of a set of institutional, technical, and physical safeguards that preserve the right to privacy with respect to the

guidance for humanitarians, they do not specifically address the issue of data sharing with donors – nor how humanitarian organisations and donors subject to different policy and legal frameworks can balance accountability, transparency, and data protection in principled humanitarian action.

Much like humanitarians, donors have developed different frameworks to inform a common approach to their work. The Good Humanitarian Donorship Initiative's (GHDI) Principles and Good Practice of Humanitarian Donorship[15] is one of the most widely endorsed frameworks of reference for donors in the sector. Unfortunately, perhaps because it pre-dates the recognition of data protection and data subject rights as fundamental to principled humanitarian action, the GHDI framework is silent on how donors' management of and requests for data relate to accountability and transparency. Another document, the Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming,[16] addresses a range of issues related to how humanitarians manage data but fails to address open questions around data sharing between humanitarians and donors, as does the Grand Bargain's 8+3 reporting template.[17] The latter is useful for minimising data collection, but does not address data protection in data sharing per se.

The Principled Framework for Responsible Data Sharing Between Humanitarian Organisations and Donors, produced through the HDTI dialogue process, sought to address these gaps while building on the foundational frameworks for the sector.[18] The substance of the Framework and related efforts to advance its use are examined later in the chapter. First, we turn to the practical dynamics of data sharing between humanitarians and donors.

---

processing of personal data and uphold the rights of data subjects. 'Data security', which is applicable to both personal and non-personal data, refers to physical, technical, and procedural measures that aim to safeguard the confidentiality, availability, and integrity of data.

15 "24 Principles and Good Practice of Humanitarian Donorship, Good Humanitarian Donor Initiative," accessed 3 May 2025, https://www.ghdinitiative.org/assets/files/GHD%20Principles%20and%20Good%20Practice/GHD%20Principles.pdf.

16 Donor Cash Forum, *Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming*, (CALP, 2022), https://www.calp-network.org/publication/donor-cash-forum-statement-and-guiding-principles-on-interoperability-of-data-systems-in-humanitarian-cash-programming/.

17 "The 8+3 Template: Key Information on the New Harmonized Reporting Standard," accessed 16 May 2025, https://gppi.net/assets/4pager_83_final_A4.pdf.

18 "A Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors", HDTI, accessed 3 May 2025, https://centre.humdata.org/a-principled-framework-for-responsible-data-sharing-between-humanitarian-organizations-and-donors/.

(In)formal Dynamics and Risks of Data Sharing in Practice

Research commissioned as part of the HDTI dialogue process about the formal and informal practices governing data sharing between humanitarian organisations and donors[19] reveals significant variations as well as exceptions and complications.[20] The research specifically examined the formal and informal frameworks that govern this type of data sharing, and how these frameworks and related requirements were understood and implemented by different stakeholders. It also retrieved and reviewed dozens of internal guidelines and instructions on data sharing, much but not all of which are publicly available.[21] This highlighted one of the major challenges of understanding and navigating this issue: the opacity and shifting sands of how data sharing is governed in humanitarian action.

Formal requests for data tend to be included in grant agreements to provide project or programme funding or, for larger agencies, in country-level or bilateral 'framework agreements', with the former applying to non-governmental organisations (NGOs) and the latter applying to UN agencies, large international NGO partners, or the ICRC.[22] Such data requests tend to be negotiated at the outset of a partnership and are usually made in writing and scheduled in advance. Project or programme agreements tend to include more frequent and detailed data sharing requests in comparison to framework agreements. These formal requests are often cyclical, related to programme cycles and financial reporting, and are mandatory, linked to compliance with existing law or policy (e.g. safeguarding policies, anti-fraud/anti-corruption). Much of this data is disaggregated and non-personal (e.g. descriptions of programme activities or household-level survey results), although some sharing of personal data may be required for monitoring and evaluation purposes,

19 Unless otherwise specified, the findings from this section are summarised from the following publications and related primary research: Fast, "Data Sharing"; and Fast, "Governing Data: Relationships, Trust, and Ethics," *Daedalus* 152, no. 2 (2023): 125–140, https://doi.org/10.1162/DAED_a_01996. More information about the methodology, which included a review of approximately 70 relevant data sharing documents (agreement templates and contracts, data policies and guidance, and reporting templates) as well as 27 interviews, is available in Fast, "Data Sharing," 8–9.

20 Importantly, the research did not address data sharing with host States or non-humanitarian actors (e.g. military or private sector actors), which raises separate concerns beyond the scope of this chapter.

21 When the HDTI commissioned this research in December 2020, only USAID and GIZ had publicly available guidelines on data sharing. See USAID, "Considerations for using data responsibly at USAID," (USAID, FHI360 and mSTAR, 2019), https://merltech.org/wp-content/uploads/2025/05/2019-USAID-UsingDataResponsibly-FINAL-2019.pdf; GIZ, "Data Protection," accessed 20 May 2025, https://www.giz.de/en/html/data_protection.html.

22 Fast, "Data Sharing," 18–19.

such as to document fraud or to prevent sexual exploitation and abuse (e.g. names and addresses of recipients of assistance).[23]

This does not mean that there are no risks or complications with formal requests for data, however. Data sharing in formal agreements is often governed by vague and generic references to "data", with no shared or consistent use of terminology. For instance, "data" could refer to everything from personal data about individual aid recipients or staff members (as in the case of safeguarding requests) to financial or context-related information (e.g. security incidents) and programme-related indicators, even though different legal and regulatory frameworks apply to these types of data. The lack of specificity is linked to risks related to the use of data for non-humanitarian purposes,[24] such as counterterrorism screening (as explained above), to track migration movements, or for commercial purposes.[25] In other cases, there is a concern that sharing data with donors could lead to humanitarian data being used in service of intelligence gathering, potentially leading to reputational and operational risks for the humanitarian organisation as well as undermining humanitarian principles of neutrality and independence. Although donors recognised such concerns in theory, they were generally unaware of such uses in practice.[26]

Informal requests concern information or data that typically fall outside of the prescribed project cycle or usual scope of reporting. These *ad hoc* requests often carry implicit value, meaning that while they are not formally required, delivering this supplementary data is deemed beneficial for an organisation's ongoing engagement and partnership with a donor. The informal requests that occur tend to be context-related, such as situational analysis to inform a donor's understanding of a dynamic humanitarian response, or in response to internal queries, such as legislative or executive body audits and reviews. For instance, a donor may request information about recent security incidents to better understand conflict dynamics, or may request more detailed financial or aid recipient information to comply with a parliamentary committee query. These requests represent a dilemma for humanitarian actors: refusing could put a relationship at risk and complying may require sharing personal or sensitive data.

The lack of specificity around data in both formal and informal requests and related guidance can lead to inconsistent practices and expectations across donors and humanitarian partners. The research pointed to different

23 For more specifics about the types of data shared, see Fast, "Data Sharing," 10, 12.

24 ICRC, "Safeguarding Humanitarian Data: Background Document," 2022, accessed 16 May 2025, https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf.

25 Westphal and Meier, "Research on the Specific Risks," 8–9.

26 Fast, "Data Sharing," 17.

standards and practices applied to partners and underscores the need to define the parameters of the "data" under discussion. For example, many donors require independent evaluation of project activities, hiring external "third-party monitors" – other NGOs, consultants, or private sector actors – to conduct these evaluations. These monitors, in turn, request personal data from humanitarian organisations to carry out their evaluations, and often hire in-country organisations to collect data. Even though formal agreements may include mandatory data sharing for evaluation purposes, each of these actors may have different approaches or abilities to protect personal data. Moreover, the type of data to be shared may not be specified in these formal agreements, nor is this type of sharing typically included since it refers to indirect data sharing.[27] Thus, data sharing guidance in relation to third-party monitors and in service of operational coordination activities in a country remains opaque.[28]

The research identified a lack of data literacy and awareness of data management risks among both donors and humanitarians. Poor data literacy may mean individuals are not attuned to the vulnerabilities and potential risks of their data practices. As noted above, re-identification is an oft-cited risk of collecting personal data, but this risk decreases (but does not necessarily disappear, even with group data)[29] when data is shared in aggregate formats.[30] Likewise, at a basic level, data shared must first be collected; the two processes are inherently linked. More requests to share data implicitly and explicitly promote further data collection, thereby increasing the risk of data exposure. This is especially true in cases with complex chains of data custody. Similarly, the mechanisms to collect, store, and share personal data, whether on spreadsheets or via blockchain or biometrics, if not well understood, can intensify risk, particularly where these mechanisms require extensive technical or legal expertise.[31] A lack of data literacy exacerbates each of these risks.

The same concern extends to risks related to data retention and destruction. This is particularly relevant in 2025 considering the major aid cuts and resulting rapid draw-down of many humanitarian operations – a trend that looks likely to continue. Data protection risks often manifest with data being

27 Fast, "Data Sharing," 15 and 23; Westphal and Meier, "Research on the Specific Risks," 8 and 13.

28 Fast, "Data Sharing," 16; Westphal and Meier, "Research on the Specific Risks," 7.

29 Linnet Taylor, "Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World," in *Group Privacy*, ed. Linnet Taylor, Luciano Floridi, and Bart van der Sloot, (Springer, 2017 vol. 126), https://doi.org/10.1007/978-3-319-46608-8_2.

30 See also Westphal and Meier, "Research on the Specific Risks," 7.

31 Fast, "Governing Data," 135.

"left behind" following the sudden[32] or planned[33] closure of humanitarian programmes, creating a situation where personal or otherwise sensitive data could be shared without adequate protection or fall into the possession of non-humanitarian actors.[34] These risks highlight the importance of specifying terms for data retention and destruction as integral to data protection efforts when sharing data with donors. Unfortunately, such terms are rarely included in standard donor agreements or monitored as part of grant or programme closure.

Complications and Challenges for Data Protection in Data Sharing

The issues discussed above – particularly the inconsistencies of expectations and practices and the intricate connection between requests and sharing – highlight a range of complications and challenges. We address these under two themes: complexities of compliance and asymmetries in power and trust.

The Complexities of Compliance

Most donors and humanitarian organisations are subject to legal and regulatory frameworks governing the protection of personal data.[35] Each partner may have different obligations that need to be observed. Multiple and overlapping regulatory frameworks create complications and uncertainty regarding compliance and may impose contradictory obligations. The articulation of the personal data protection principle in the IASC Operational Guidance on Data Responsibility summarises this complexity of compliance well:

32 Katja Lindskov Jacobsen and Karl Steinacker, "Contingency Planning in the Digital Age: Biometric Data of Afghans Must Be Reconsidered," *PRIO Blogs*, 26 August 2021, https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/.

33 Matthew Hunt, Isabel Muñoz Beaulieu, and Handreen Mohammed Saeed. "What Does 'Closing Well' Entail for Humanitarian Project Data? Seven Questions as Humanitarian Health Projects Are (Being) Closed or Handed Over," *Journal of Humanitarian Affairs* 5, no. 2 (2023): 13–23, accessed 3 May 2025, https://doi.org/10.7227/JHA.106.

34 Since the research was published, the circumstances related to the closure of USAID raise questions about the protection of data collected for humanitarian purposes. See Sylvia Thomson, "US federal workers clamp down on their communications in climate of DOGE-induced fear," *CBC.ca*, 19 March 2025, https://www.cbc.ca/news/world/usaid-doge-signal-1.7487269.

35 For more on the varied legal and regulatory frameworks to which humanitarian organisations are subject, see Chapter 8, "Legal tensions: insights from the UN-EU correspondence on EU data protection law and the role of privileges and immunities as a catalyst for enhancing personal data protection".

> When managing personal data, humanitarian organizations have an obligation to adhere to applicable national and regional data protection laws, or (ii) if they enjoy privileges and immunities such that national and regional laws do not apply to them, to their own data protection policies.[36] These laws and policies contain the principles for personal data protection, such as a list of equally valid legal bases for the processing of personal data, including but not limited to consent.[37] Humanitarian organizations subject to national or regional legislation should also take into account the guidelines and advisories issued by relevant data protection authorities within their applicable jurisdiction.[38]

Alongside data protection, donors are also subject to varied political, legal, and statutory requirements related to counterterrorism, migration management, and law enforcement, amongst others. In many cases, donors might want to use data shared by humanitarian partners to verify their compliance with these different requirements. Some donors include counterterrorism clauses in their grant agreements, which are intended to ensure that their funds are not used to benefit designated terrorist groups.[39] In order to ensure compliance, donors might request highly disaggregated data to corroborate their due diligence processes, ensuring their partners are not engaging with any "sanctioned person or entity". Similarly, donors might include clauses to cover safeguarding, anti-bribery, anti-fraud, and anti-corruption measures.[40]

36 In respect of UN-system organisations, the High Level Committee on Management adopted the Personal Data Protection and Privacy Principles, which should serve as a foundational framework for the processing of personal data by UN entities. For organisations that do not enjoy privileges and immunities, reference should be made to applicable data protection legislation as well as sets of principles and other guidance which such organisations are subject to. (N.B.: this footnote is from the original text in the IASC Operational Guidance, 2023).

37 Humanitarian organisations may not be in a position to rely on consent for all personal data processing. For further details about the legal bases for personal data processing, see the ICRC Handbook on Data Protection in Humanitarian Action (2nd edition, 2020), https://www.icrc.org/en/data-protection-humanitarian-action-handbook. Regardless of the selected legitimate basis, data subject rights ensure the agency and involvement of individuals with regard to how their personal data is processed. (N.B.: this footnote is from the original text in the IASC Operational Guidance, 2023).

38 Data Responsibility Working Group, "Operational Guidance: Data Responsibility in Humanitarian Action," (IASC, 2023), 18, accessed 16 May 2025, https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf .

39 "Toolkit for Principled Humanitarian Action: Managing Counterterrorism Risks," Norwegian Refugee Council, accessed 16 May 2025, https://www.nrc.no/shorthand/stories/toolkit-for-principled-humanitarian-action/index.html.

40 Justine Walker, "Risk Management Principles Guide for Sending Humanitarian Funds into Syria and Similar High-Risk Jurisdictions, 2020," https://www.graduateinstitute.ch/sites

A balancing of the potentially competing interests served by these requirements and donors' own data protection laws and related obligations is another source of complexity. The extant instructions on data sharing and related practice suggest that this balancing is not something with which donors have proactively grappled to-date.[41]

Even when there is clarity between donors and humanitarians regarding the compliance requirements for data protection in data sharing in a particular collaborative relationship or crisis context, compliance remains challenging due to gaps in competency, capacity, and capability for both parties.[42] One clear example of this is the now quite standard requirement of Data Protection Impact Assessments (DPIAs) in scenarios where personal data is being managed (and potentially shared). While the spirit for such a requirement is willing, experience suggests the flesh is still weak. When done well, DPIAs are essential tools for identifying and mitigating data protection risks. All too often, however, they are treated as a formality, rather than as a substantive process to identify and mitigate risks to data subjects.[43] Most donors and humanitarian organisations still lack the competency, capacity, and capability to conduct comprehensive DPIAs, leading to assessments that are incomplete or sometimes not conducted at all. Without clear and well-resourced mechanisms to ensure compliance, foundational requirements such as DPIAs risk being treated as red tape to be cut rather than as meaningful measures for protecting personal data.

Asymmetries in Power and Trust

The practicalities of data sharing between humanitarians and donors offer a lens through which to examine the asymmetric power dynamics of the sector.

/internet/files/2020-05/26-MAY-SYRIA-Risk%20Management%20GuideFINAL.pdf. "Sanctioned persons" may include individuals, terrorist groups, governments, as well as companies and other entities of legal personality. VOICE, "The Impact of EU Sanctions and Restrictive Measures on Humanitarian Action," Workshop Report, November 2019, https://voiceeu.org/publications/voice-workshop-report-the-impact-of-eu-sanctions-and-restrictive-measures-on-humanitarian-action.pdf.

41 The Global Privacy Assembly Working Group on the Role of Privacy in International Development Assistance, International Humanitarian Assistance and Crisis Management (WG AID) would be an ideal forum to examine this complexity in compliance in more detail. For more on the role and work to-date of this group, see Lennman in this volume.

42 For more on the notion of competency, capacity, and capability vis-a-vis humanitarian data and information activities, see Stuart Campo et al., "Signal Code: Ethical Obligations for Humanitarian Information Activities," (Harvard Humanitarian Initiative, 2018), https://hhi.harvard.edu/sites/g/files/omnuum6866/files/humanitarianinitiative/files/signal_obligations_final_05.24.2018.pdf; Fast, "Data Sharing," 19.

43 Massimo Marelli ed., ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition, Cambridge, 2024, https://doi.org/10.1017/9781009414630.

Many donors recognise that their data sharing requests tend to advance their own priorities rather than promoting evidence-based programming to increase effectiveness, even as some of the requests are driven by the desire to gather evidence. This increases the amount of data collected even if not all is used, contravening a key tenet of data protection. As one donor recognised, data requests may not be "fit-for-purpose" in that they better assist donor decision-making instead of serving "as a tool for partners to make evidence-based adjustments in programming".[44] Thus, in practice, the sharing or flow of data between humanitarians and donors tends to be vertical and upward (from project recipients and local data collectors to donors), usually in response to requests that move downward (from donors to humanitarian organisations).

As discussed above, this sharing is both formal and informal, varying by donor and context. In some cases, donors request specific and detailed programmatic data, potentially including personal data, while in others a more general narrative with aggregated, categorical data suffices.[45] Data sharing also occurs horizontally, usually for operational purposes such as coordination activities; this sharing often relies on more informal requests that are not regulated in legal agreements. Rarely, however, does this flow become a loop, where requests move upward or, more importantly, where the analysis and findings return to and influence the work of those providing or collecting the data. As such, the flow of data graphically illustrates the power dynamics of the humanitarian system: those with the most power in the system request the data, while those with the least power and resources (recipients of aid and local NGOs) provide or collect the data.

Relatedly, these informal and formal practices of data sharing reveal and strengthen the existing power inequalities in the system.[46] The formal framework agreements illustrate the variable standards for data sharing, requiring more specific data sharing from the smaller project-level agreements (usually with NGOs) and allocating the most flexibility to the biggest organisations with the largest budgets. Thus, the UN and large humanitarian organisations, which have longstanding relationships with donors, have the most leverage in negotiating data sharing requests. This is a result of both the type of contract (framework agreements, which tend to set broad parameters for action and for data sharing) and a level of trust built over years of repeated contracts and interactions. In contrast, less internationally known actors, most often local NGOs, typically have the most onerous requirements placed on them, in order to "prove" their responsiveness and trustworthiness. The ability of all humanitarians to refuse data sharing requests, however, typically depends on

44 Fast, "Data Sharing," 16.
45 Fast, "Data Sharing".
46 Fast, "Data Sharing," 18, 22–23; Fast, "Governing Data," 134–136.

the donor requesting the data, the organisation's reliance on that particular donor for ongoing or future funding, and the sensitivity of the request; these decisions often fall to senior management or donor relations teams, and not programme teams.[47] This raises questions about the place and continued relevance of humanitarian principles – particularly independence – in relation to data sharing.

Another complication stemming from these power dynamics relates to the scrutiny placed on donors and its impact on the data they request. Multiple donors highlighted how instances of fraud or corruption in the humanitarian sector tended to increase scrutiny of their own actions. This then resulted in more requests to partners to share data to provide the requisite assurances that funds were not misused.[48] Likewise, scrutiny could be linked to data breaches, such as the UN sharing Rohingya refugee data with Myanmar authorities without consent[49] or the Red Cross Family Tracing data breach discussed in this volume,[50] or to controversies affecting the humanitarian sector more broadly. For instance, after explosive media stories of humanitarians' sexual exploitation and abuse of aid recipients, public outrage and calls for more accountability have resulted in mandatory reporting, including personal data, in relation to the prevention of sexual exploitation and abuse and other safeguarding concerns. While understandable, such attention can also have the opposite effect, whereby data misuse or concerns about data quality lead to more requests to scrutinise the data collected, potentially including the sharing of personal data. This can decrease the overall trust in "humanitarian numbers" more generally.[51] Paradoxically, it also ultimately increases the amount of data collected and further heightens the risk of data breaches with particularly sensitive data.

Prospects and Pitfalls of a Common Framework for Data Sharing Between Humanitarians and Donors

In response to the complex dynamics and challenges described above and drawing on the insights and inputs of a cross-section of major humanitarian organisations and donors over two years of research and consultation,

47 Westphal and Meier, "Research on the Specific Risks," 11–12; Fast, "Data Sharing," 19–21, 23; Fast, "Governing Data," 131.

48 Fast, "Data Sharing,"; Fast, "Governing Data," 134–135.

49 Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent: Bangladesh Provided Myanmar Information that Refugee Agency Collected," 15 June 2021, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent. Importantly, this is an example of data sharing with a host State, not a donor.

50 Chapter 12, "By the Book, Beyond and Backwards? Ethical Considerations on the 2022 Data Breach Affecting the Family Links Network of the Red Cross and Red Crescent Movement".

51 Fast, "Governing Data," 129–130.

the HDTI issued the Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors.[52] The Framework reflects the prospects of a collective vision and common approach to upholding data protection in data sharing, as well as the pitfalls of a singular approach to this inherently complex and messy area of humanitarian action.

During the drafting phase, the Framework's lead authors debated whether to articulate a set of principles for data sharing or, rather, a set of practical actions or guidelines for data sharing that aligned with a principled approach to aid. The authors landed on the latter, offering a document "designed to reinforce the overarching commitment to 'do no harm', while minimizing the risks and maximizing the benefits of data in humanitarian action." To be sure, the challenges facing humanitarians and donors vis-a-vis data sharing are not and have never been the result of a lack of shared principles. As explained earlier in this chapter and in numerous other chapters in this volume, common principles for data protection are well recognised and supported across the humanitarian system. The devil is in the detail, specifically in their varied interpretation and implementation, which the HDTI Framework sought to address.

The issues surrounding the complexities of compliance described earlier in this chapter become clear in the following instructions in the Framework's opening objectives:

> Individual entities are encouraged to adapt this framework to their own institutional context, including through relevant guidelines, procedures, templates and tools for data sharing where appropriate. Adaptation and adoption of the framework should align with different donors' and humanitarian organizations' respective mandates, relevant legal, policy, and regulatory frameworks, and the decisions of governing bodies.

Such qualifications, while necessary, also point to the potential pitfalls of a singular framework for a network of actors as diverse and complex as the humanitarian system.

Nevertheless, the practical "guidelines" the Framework offers serve as a clear and consistent guide for how humanitarians and donors can put common principles into practice when sharing data.[53] It calls for the following:

52 Except where otherwise noted, the references in this sub-section are taken from the HDTI Principled Framework for Data Sharing Between Humanitarian Organizations and Donors, available here: https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/6841d1d2-3ba9-4a05-8802-fe29b7385f50/download/a-principled-framework-for-responsible-data-sharing-between-humanitarian-organizations-and-donor.pdf.

53 As explained in the Framework, these guidelines build directly on and complement existing principles and guidance for data protection in humanitarian action. This includes IASC

1. prioritise the rights and needs of affected populations;
2. specify and clearly communicate the purposes of data sharing and the type of data required for these purposes in a given context;
3. clarify and formalise requirements for responsible data sharing and establish appropriate agreements to support implementation in different contexts;
4. use a common approach for assessing and mitigating risks related to data sharing specific to humanitarian contexts;
5. invest in the capacity required to develop and uphold sector-wide approaches for data responsibility throughout the data lifecycle;
6. contribute to joint advocacy, learning, and development of additional guidelines for responsible data sharing.

The Framework offers concrete recommendations for each guideline targeted at both parties to inform implementation. These recommendations go much further than previous internal or sector-wide guidance in articulating clear actions to support better practice, and help balance transparency, accountability, and data protection. In this way, the Framework closes a gap for both parties related to data protection in data sharing, thereby delivering on its original aim. Unfortunately, however, the presence and recognition of a common framework do not automatically lead to better practice.

As a founding party of the HDTI and longstanding supporter of data protection in humanitarian action, Switzerland has actively promoted the Principled Framework for Responsible Data Sharing Between Humanitarian Organizations and Donors through a combination of policy integration, capacity-building activities, and external outreach. Domestically, Switzerland conducted internal training with the ICRC and OCHA and established in-house data protection champions. The HDTI was also embedded in Switzerland's Digital Foreign Policy Strategy.[54] Externally, the Framework was socialised at the Humanitarian Networks and Partnerships Weeks in 2023 and at donor meetings in Geneva. Switzerland also organised regional workshops to sensitise and engage donors and humanitarian actors. Ongoing efforts include developing data-sharing standards in contracts with humanitarian actors and promoting data protection standards in international policy forums.

Operational Guidance and the ICRC Handbook. They also account for other frameworks for principled humanitarian action, including the Good Humanitarian Donorship Initiative's 24 Principles and Good Practice of Humanitarian Donorship and the Donor Cash Forum Statement and Guiding Principles on Interoperability of Data Systems in Humanitarian Cash Programming.

54 FDFA, "Digital Foreign Policy Strategy," (Federal Department of Foreign Aid, Switzerland, 2024), accessed 16 May 2025, https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/thematische-strategien/strategie-digitalaussenpolitik.html.

Within the broader humanitarian and donor community, progress has been primarily limited to the dissemination of the Framework, with less progress made in its implementation or in changing practices related to data sharing. While research and experience suggest that the varying capacities and competing pressures on humanitarians and donors may make the adoption of a single framework challenging in practice, the intention of the Framework's authors was to foster further discussion, joint adaptation, and tailoring to promote adoption by different stakeholders and drive better practice and evolution over time. Critically, the HDTI process achieved what it set out to in terms of securing traction with senior management from both stakeholder groups. This support and continued high-level advocacy for data protection as a priority issue for the sector remain the most impactful contributions of the dialogue process and the Framework that it yielded.

In addition, increased awareness of the power differentials inherent in these frameworks and agreements creates space for better practice and collective action, such as through promoting data literacy and providing support for data protection within those organisations collecting and storing personal data. Likewise, thinking through the ways that data sharing illustrates how power manifests in the system suggests some potential options. For instance, delinking the functions of collecting data about the needs of affected populations and responding to these needs could decentralise power in the system, by requiring more data sharing among humanitarians both large and small, and by delinking data sharing requests and funding for operational activities.

Conclusion: Roll-Back or Reinvigoration – Whither Collective Action on Data Protection in Data Sharing?

In conclusion, the research and experience examined in this chapter demonstrate that the past ten years have seen deep convergence and collaboration between humanitarian organisations and donors in advancing data protection in data sharing. The HDTI dialogue process was not simply a "coalition of the willing" but a truly collaborative endeavour bringing together a diverse group of stakeholders from across the system to articulate a vision for collective action. While that vision remains intact, the commitment, drive, and resources to realise it are increasingly scarce.

To be sure, in the current humanitarian landscape, there is also a real risk of roll-back on the shared principles that underpin the Framework. As a recent report on the Good Humanitarian Donorship Initiative observes,

> Since the establishment in 2003 of the Good Humanitarian Donorship Initiative (GHDI), the world in which humanitarian donors seek to be 'good' has altered significantly: the nature of humanitarian challenges has changed; the demands on humanitarian donorship have escalated; the

> humanitarian coordination landscape has become more crowded; and yet the global respect for humanitarian norms and the geopolitical space for multilateral cooperation has diminished. ... Although the initiative has proved highly successful in attracting a diverse group of members to sign up to the principles, and in establishing an important set of norms for donor behaviour, there is a widespread sense that it requires reinvigoration.[55]

How might we maintain the momentum of the past decade and solid progress on data protection in humanitarian action against a backdrop of deep uncertainty and fragility? Will we see a roll-back in collective action on this and other issues of principled humanitarian aid, or will the crisis facing the system serve as a call for reinvigoration and redoubled collective action? Will the rapid embrace of new technologies – particularly artificial intelligence (AI) – accelerate data protection risks and amplify dataveillance,[56] or will it catalyse investment in data protection by design and by default? These questions will remain at the heart of the humanitarian data protection and data sharing endeavour.

If donors and humanitarians are to meaningfully balance accountability, transparency, and data protection in practice amidst what is arguably the greatest disruption in the history of the humanitarian sector, they must find ways to continue working together. This will require pooling resources to leverage the competency, capacity, and capability that remain for upholding data protection, allowing for better minimising risks while maximising the benefits of data. Principled humanitarian aid in an increasingly data-driven and digitalised ecosystem requires humanitarian organisations and donors to redouble their commitment to data protection, both because it enables better, more dignified aid and protection, and because it is the right thing to do.

55 Sophia Swithern, "Revitalising the Good Humanitarian Donorship Initiative: A 20-year Review," *Humanitarian Policy Group (HPG) Report*, (ODI, 2024), 7, https://odi.cdn.ngo/media/documents/HPG_report-GHD-final_JbW0Itp.pdf.

56 Kristin Bergtora Sandvik, *Humanitarian Extractivism: The Digital Transformation of Aid* (Manchester University Press, 2023).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

PART 4

Regional and Local Perspectives on Data Protection

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

16

"WITHDRAW YOUR DATA"

How Data Protection Legislation Can Reshape Humanitarian Action

Timothy Charlton and Cassie Jiun Seo

Introduction

Data Protection Legislation (DPL) is fundamentally reshaping power dynamics within humanitarian action, especially in the context of operations that rely on digital tools to collect and process aid recipients' personal data. As DPL is rolled out globally through country-specific or multinational lawmaking, many humanitarian actors find themselves operating under or, in the case of international organisations (IOs), interacting with a regional or even multiple overlapping DPL frameworks,[1] which furnish subjects with considerable rights, including access, rectification, or removal of their personal data. Humanitarian organisations have adopted data protection frameworks codifying their data protection standards and commitments and extending rights to the affected populations they serve. In the case of IOs, these frameworks substitute national and international DPL.

Exercising data rights, especially the 'right to erasure / right to be forgotten', could empower aid recipients to control their personal data, including the ability to restrict processing by data controllers (aid agencies), thus significantly altering the positionality of the parties involved in humanitarian aid. Evidence is gradually emerging on how DPL affects humanitarian organisations' capacity to operate and on how affected populations understand their rights vis-à-vis

1 Analysing how the introduction of DPL affects humanitarian organisations has important implications for the sector. For example, it raises the question of what, if any, action organisations exempted from regionally specific DPL through their privileges and immunities should take to avoid a divergence in recipients' rights between aid providers.

DOI: 10.4324/9781003650164-23

humanitarian aid providers.[2] Navigating this complex regulatory landscape, including regional differences, organisational commitments, and increasingly digitally literate affected populations,[3] while ensuring data protection and retaining full operational capacity is a pressing challenge for the principles-driven sector. Humanitarian action today is increasingly digital,[4] and as aid recipients become more aware of their data rights, they can challenge prevailing top-down "extractivistic"[5] approaches to personal data handling in humanitarian digital interventions. Social media platforms often play a crucial role in organising and amplifying these demands, acting as public sounding boards and accountability channels that pressure organisations to comply with DPL requirements. Simultaneously, the centrality of social media in some digital humanitarian operations, especially related to feedback and requests for deletion or modification of personal data under DPL, presents a risk factor, due to social media platforms' centralised ownership and opaque algorithmic curation practices.

This chapter investigates how DPL plays out in contemporary humanitarian action using a mixed-method approach. We briefly discuss DPL applicability in humanitarian situations and how its presence might shape perceptions and expectations in affected populations. We then describe a single embedded case study[6] of documented data deletion requests during the early phases of

2 Nathan Clark and Kristoffer Albris, "In the Interest(s) of Many: Governing Data in Crises," *Politics and Governance* 8, no. 4 (2020): 421–431, https://doi.org/10.17645/pag.v8i4.3110; Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and "Big Data,"" *International Review of the Red Cross* 99, no. 904 (2017): 179–209, https://doi.org/10.1017/S1816383117000637.

3 Despite being a global trend, regional differences and a digital divide remain, with several locations in Africa showing low overall digital literacy. "Digital Skills in the Global South: Gaps, Needs, and Progress," GIGA Focus Global, 2023, https://www.giga-hamburg.de/en/publications/giga-focus/digital-skills-in-the-global-south-gaps-needs-and-progress; UN Women, "Innovation and Technology in Humanitarian Settings," (2023), accessed 3 June 2025, https://asiapacific.unwomen.org/sites/default/files/2023-02/ap-Good-Practices--Innovation-and-Technology-in-Humanitarian-Settings.pdf.

4 "The State of the World's Cash 2023. Chapter 2: CVA Volume and Growth," The CALP Network, accessed 10 May 2025, https://www.calpnetwork.org/web-read/the-state-of-the-worlds-cash-2023-chapter-2-cva-volume-and-growth/.

5 Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi, "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data," *Environment and Planning D* 34, no. 6 (2016): 990–1006, https://doi.org/10.1177/0263775816633195; Kristin Sandvik, *Humanitarian Extractivism: The Digital Transformation of Aid*, Humanitarianism Key Debates & New Approaches (Manchester: Manchester University Press, 2023); Kristin Bergtora Sandvik, "Wearables for Something Good: Aid, Dataveillance and the Production of Children's Digital Bodies," *Information, Communication & Society* 23, no. 14 (2020): 2014–2029, https://doi.org/10.1080/1369118X.2020.1753797.

6 Robert K. Yin, *Case Study Research: Design and Methods*, 3rd ed, Applied Social Research Methods Series, vol. 5 (Thousand Oaks: Sage Publications, 2003), 23.

the full-scale invasion of Ukraine by the Russian Federation in 2022,[7] when some humanitarian organisations relied heavily on digital technologies, such as social media chatbots, to facilitate their cash-based responses.[8] Based on a sample collected from mixed primary and secondary data sources, we map the motivations behind data-deletion requests by recipients of humanitarian aid and elicit how DPL compliance shapes humanitarian responses. Finally, we outline how the presence of DPL could impact future humanitarian operations and formulate policy recommendations to increase digital preparedness in the sector. By presenting this research, we contribute further evidence to a rapidly evolving and operationally critical aspect of contemporary humanitarian action in an area where empirical research is so far scarce.

Method and Data

This chapter draws on mixed research methods and data collected using an opportunistic sampling strategy (Table 16.1). First, we conducted qualitative key-informant interviews (KIIs) (n=3) with experts from the humanitarian sector, who described the gradual changes introduced through DPL. Interviews were recorded, transcribed, and subsequently analysed for relevant insights. As the contours of the case study emerged, we collected further KIIs from participants with direct experience of the local situation (n=2). Second, we manually collected supplementary documents and social media data from the presence on the Facebook social media platform of a major humanitarian non-governmental organisation (NGO) involved in the humanitarian response in Ukraine (n=149). This data was stored in a database, automatically translated to English where applicable, and analysed together with the interviews.

Our analysis follows a single embedded case study approach[9] centred around observation on DPL deletion requests and drawing in additional sources and documentation as required. A single case approach to a case study research design depends on the convergence of evidence from multiple sources to establish a circumstance. In this case, our aim is to establish 1) how

7 We align our wording with that used recently by the UN Office for the Coordination of Humanitarian Affairs (OCHA) and by the United Nations High Commissioner for Refugees (UNHCR): UNHCR, "Ukraine," accessed 11 June 2025, https://www.unhcr.org/where-we-work/countries/ukraine; OCHA, "Ukraine: Summary of the Humanitarian Needs and Response Plan and the Regional Refugee Response Plan (January 2025)," 16 January 2025, https://www.unocha.org/publications/report/ukraine/ukraine-summary-humanitarian-needs-and-response-plan-and-regional-refugee-response-plan-january-2025-enuk.

8 Diana Tonea and Vicente Palacios, "Registration, Targeting and Deduplication: Emergency Response inside Ukraine," Thematic Paper (CALP Network, 2022), https://www.calp-network.org/wp-content/uploads/2022/09/Registration-Targeting-and-Deduplication-Emergency-Response-inside-Ukraine-Thematic-paper-1.pdf.

9 Yin, *Case Study Research*, 23.

TABLE 16.1 Data Sources

Type	*n*	*Description*
KIIs	5	Qualitative interviews with practitioners directly involved in the early phase of the Ukraine humanitarian response or domain experts on DPL in other humanitarian contexts
Social media data	149	Posts manually collected from a major humanitarian organisation's Facebook page; machine translated from Ukrainian or Russian to English
Archival document analysis	3	Documents outlining the early humanitarian intervention in Ukraine and technical documents related to DPL applicability (report, vacancy announcement, website snapshot)
Doctrinal analysis	3	Analysis of legal texts and relevant supplementary documents, such as model grant agreements

recipients of humanitarian aid enforce accountability through data subject requests enabled by DPL and 2) what motivates these requests. Individual data subject requests therefore form the units of analysis in our research design, and they are substantiated from both the recipients' side (documented through social media data) and the providers' side (through KIIs). In a final section, we discuss the implications of our findings for humanitarian organisations in current and future operations. We emphasise that our findings and the case study are not representative of the humanitarian response in Ukraine, as this was not our research aim. Instead, we sought to highlight a salient 'edge case' that illustrates how, in some (but not all) situations, the expectations and perceptions of affected populations around their data and their legal rights under DPL or comparable data protection frameworks are affecting the power dynamics between recipients and providers of humanitarian aid. By documenting this case, this research provides insights into a highly relevant phenomenon in contemporary humanitarian action. By studying how DPL is empowering aid recipients to hold humanitarian organisations accountable, important lessons for humanitarian preparedness and future research can be drawn.

This study has some limitations. First, the sensitive nature and ongoing armed conflict in the area under study made data collection prohibitively difficult and we had to resort to a convenience sampling approach, drawing all potentially relevant data sources into the study as they became available. This means the research is potentially over-reliant on a limited number of individual accounts and should be repeated with a larger, more diverse sample. Second, ethical concerns prohibited us from contacting affected individuals directly, e.g. using the social media channels where they aired frustration and

organised responses. Such research would be highly valuable and the possibility of ethically compliant research with affected populations should be carefully evaluated. Third, while a single case study approach can highlight emerging tensions or dynamics, an expanded research design covering multiple humanitarian contexts will be necessary to show the global effect of DPL on humanitarian action.

Analysing the Applicability of DPL in Humanitarian Action

Humanitarian organisations, particularly NGOs, increasingly operate in complex environments where multiple DPLs intersect. These actors often work across borders, handling the personal data of vulnerable populations under diverse privacy regimes. Compliance is complicated by operational realities on the ground, where legal standards often trail digital innovations. Additionally, many humanitarian NGOs partner with IOs, which typically benefit from privileges and immunities under international law and adopt their own binding regulatory frameworks related to data protection. IOs are considered exempt from national legislation and multinational DPL frameworks such as the EU's General Data Protection Regulation (GDPR).[10] In contrast to IOs, NGOs and other humanitarian actors must carefully navigate the growing patchwork of applicable national and international data protection requirements globally. At the same time, affected populations may become sensitised to the exercise of their data subject rights without knowing the specific mechanisms through which they would apply in their interactions with a humanitarian actor.

A further impact of the GDPR is that it is widely recognised, regardless of which DPL or data protection framework is applicable. We hypothesise that its extraterritorial reach and wide recognition contribute to a general awareness of data rights in affected populations, at least in the current case, alongside a more clearly defined national DPL. The case study presented illustrates how such heightened awareness about data rights could play out in future humanitarian encounters.

Participants in our research interviews, who held senior roles at a provider of humanitarian aid in Ukraine, corroborated this understanding of the wide

10 Christopher Kuner, "The GDPR and International Organizations," *AJIL Unbound* 114 (2020): 15–19, https://doi.org/10.1017/aju.2019.78; Christopher Kuner, "International Organizations and the EU General Data Protection Regulation: Exploring the Interaction between EU Law and International Law," *International Organizations Law Review* 16, no. 1 (2019): 158–191, https://doi.org/10.1163/15723747-2019008; Massimo Marelli, "The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders," *Computer Law & Security Review* 50 (2023): 105849, https://doi.org/10.1016/j.clsr.2023.105849.

normative and legal reach of the GDPR and other DPL. One participant claimed that "[…] if an organisation is a recipient of EU funding, they legally should be applying GDPR principles to their data collection and data management. Unless of course, they're a UN agency …" (KII participant 2), pointing out the prerogative of IOs to set and enforce their own data protection frameworks. The participant further expanded on the topic by clarifying that in their understanding, "if your funding is, let's say, from USAID through a US office [then] that project [needs to] abide by [local law]. And then if they have another project, let's say through Germany from ECHO for instance … you know, then [...] in that project we have to apply GDPR" (KII participant 2). Irrespective of the accuracy of this claim, this highlights that it is easily conceivable that upon taking up operations in a specific context, humanitarian organisations could become subject to various, potentially overlapping, DPL as a result of funding governments' contractual requirements on grants agreements and other, e.g. internal, data protection frameworks.

In general, regardless of which DPL or framework is applicable, modernised approaches will furnish data subjects with certain rights, including a right of access, rectification, and deletion.[11] Ukraine, which serves as the case study for this chapter, the Law on Personal Data Protection[12] governs the handling of personal data and establishes rights for individuals.[13] However, in situations where multiple DPLs apply, organisations might opt to align with the stricter framework to avoid complications.[14] A common experience for humanitarian actors of all colours is that they find themselves confronted with a population that is increasingly sensitised to issues of data protection without necessarily knowing its details or mechanisms. We posit that the regulatory landscape and evolving perceptions and expectations amount to a two-pronged reconfiguration of the reality of humanitarian action.

11 Baseline requirements are specified in the Council of Europe's Convention on Human Rights and Fundamental Freedoms (Convention 108+); see also, Chapter 10, "The Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+) and International Organisations".

12 "The Law of Ukraine: About the Protection of Personal Data," 2010, https://natlex.ilo.org/dyn/natlex2/natlex2/files/download/87898/UKR-87898%20(EN).pdf.

13 Efforts to harmonise Ukrainian DPL with GDPR and Convention 108+ are currently underway in the Ukrainian legislative system.

14 This speculation was made by a participant in our study: "What we advocate for is that all global organisations should have […] at a bare minimum […] their own data protection and privacy policy. But that policy should abide by the kind of most stringent regulations globally". (KII participant 2)

Case Study: Ukraine

In this section, we present a case study of how the presence of DPL enabled affected individuals in Ukraine to request the removal of their data from humanitarian actors. As shown above, the applicability of DPL and data protection frameworks in humanitarian settings can be complex, though it is reasonable to expect normative alignment among humanitarian actors and a general awareness of data subject rights in the affected population. Therefore, we do not make further assumptions about the exact mechanism by which humanitarian actors would be required to comply with data subject requests but operate under the assumption that the individually applicable DPL would regulate such cases.

First, we set the scene by describing the background and context of the early-onset humanitarian operations following the 2022 full-scale invasion of Ukraine by the Russian Federation. We focus particularly on the digital ecosystem employed by humanitarian organisations, which involves numerous third-party services and platforms. Then, we introduce evidence for data subject requests made to humanitarian organisations and provide four speculative motivations that underpin them. This case study presents only a momentary and non-exhaustive snapshot of a single humanitarian context. It documents that a new dynamic between the recipients and providers of humanitarian aid is emerging due to recipients' rights to have their data modified or deleted but makes no assumptions about its scale.

Background: The Early Humanitarian Response in Ukraine

The humanitarian response following the full-scale invasion of Ukraine by the Russian Federation in 2022 stood out for its unprecedented level of digitalisation compared to previous international crises. This was driven by a combination of factors, including the widespread availability of digital infrastructure, high digital literacy among the population partially due to Ukraine's pre-war success in the information and communications technology sector, and the active role of the Ukrainian government as a key decision-maker in coordinating humanitarian efforts within its borders.[15] The response also saw the large-scale involvement of technology companies in humanitarian activities and was backed by unprecedented levels of funding from institutional donors, philanthropies, and individuals.

Within this broader digitalised landscape, cash and voucher assistance (CVA) played a central role in terms of scale and innovation. Over six

15 Renata Kurpiewska-Korbut, "Digital technologies in the global humanitarian sector: A case study of Ukraine," *Journal of Modern Science* 6, no. 60 (2024): 730–747, https://doi.org/10.13166/jms/199490

million individuals were reached in 2022, and 5.3 million in 2023, primarily through Multi-Purpose Cash Assistance (MPCA), a flexible form of assistance intended to cover essential household needs. The design and delivery of CVA in Ukraine reflected a complex and collaborative ecosystem, involving UN agencies, Red Cross and Red Crescent societies and organisations, international and local NGOs, donors, and the Ukrainian government, coordinated through the Ukraine Cash Working Group (CWG).

The MPCA delivery model at a high level encompassed the following stages: 1) initial coordination and needs assessment through the CWG; 2) targeting, outreach and registration using a combination of sources, including government-provided referral lists, field teams, and digital platforms; 3) deduplication and eligibility verification, often using Tax Identification Numbers (TINs); 4) distribution of cash assistance, primarily via (digital) bank transfers; and 5) ongoing monitoring, complaint resolution, and feedback mechanisms. Although coordination mechanisms were present, each implementing organisation largely managed its own outreach and registration pathways. For instance, one NGO used WhatsApp to register households remotely,[16] requiring submission of sensitive personal data, such as passport information or TINs, for eligibility checks. Meanwhile, the CWG, the UN Office for the Coordination of Humanitarian Affairs (OCHA), and the Emergency Telecommunications Cluster (ETC) deployed Telegram and Viber chatbots[17] to provide unidirectional information to affected communities.

Social media played a critical role across the MPCA delivery chain, supporting outreach, onboarding, one/two-way communication, and complaint resolution. Social media tools enabled direct engagement with affected populations and facilitated access to services outside traditional humanitarian structures and were described as "democratising" humanitarian action by allowing affected individuals to access and respond to aid processes outside formal systems.[18]

When humanitarian operataions scaled up in response to large-scale displacement in Ukraine, the national social protection system was widely operational, meaning humanitarian actors operated in a complementary role instead of fully replacing State-provided services.[19] As non-EU and non-European

16 Tonea and Palacios, *Registration, Targeting and Deduplication*.

17 Ukraine CWG and ETC *Humanitarian Info UA Chatbot to inform affected population about the Multipurpose Cash Assistance* (2025), https://reliefweb.int/report/ukraine/humanitarian-info-ua-chatbot-inform-affected-population-about-multipurpose-cash-assistance-enuk.

18 Romina Bandura and Janina Staguhn. "Digital Will Drive Ukraine's Modernization," Center for Strategic and International Studies, 2023, https://www.csis.org/analysis/digital-will-drive-ukraines-modernization.

19 Ground Truth Solutions, "Aligning Aid: Recipient Perspectives on Humanitarian Cash and Social Protection in Ukraine," (2024), https://www.calpnetwork.org/wp-content/uploads/2024/04/GTS_Ukraine_CCD_Round-2-report_2024_EN.pdf.

Economic Area (EEA) residents, Ukrainians do not fall directly under the GDPR's territorial scope (they could be covered, however, in their interaction with EU-linked entities). Instead, Ukraine has adopted its own DPL.[20] Moreover, compared to other humanitarian contexts, Ukraine's population demonstrates relatively high levels of digital literacy[21]. One participants in our study claimed that this extended to a well-developed awareness of digital risks, stating that: "there is a heightened awareness [in Ukraine] and a heightened kind of … you know, understanding of risk that's involved in digital space" (KII participant 2).

Registration Process of an International Humanitarian NGO

At the onset of the deployment in Ukraine, there was a genuine enthusiasm amongst the staff at the international NGO,[22] particularly about leveraging new partnerships with major technology companies and the potential of enhancing the efficiency of aid delivery and the implementation of a cash distribution programme on a larger scale than the organisation's usual portfolio. The organisation implemented a remote, digital registration system, primarily structured as a self-administered chatbot form hosted on WhatsApp. Applicants were required to provide a range of sensitive personal data, including tax and social security details, full names, phone numbers, and bank account details, along with location information shared through WhatsApp's location feature to verify displacement status (internally displaced or refugee).[23] Registrants were also asked to upload photographs of identity documents to facilitate identity verification. While the system offered scalability and rapid reach, significant operational delays emerged. The timeline from registration to the disbursement of cash assistance into recipients' bank accounts was extended by several months, largely due to procurement bottlenecks, coordination challenges, and broader systemic delays common in humanitarian operations. This occasionally led to frustration among the recipient population, as expressed by one individual: "[...] How long to wait

20 "The Law of Ukraine: About the Protection of Personal Data".

21 With only around one in nine individuals exhibiting no digital skills in 2021: DIIA, "Digital Literacy of the Population of Ukraine: Report on the Results of the National Survey," https://osvita.diia.gov.ua/uploads/0/2623-research_eng_2021.pdf.

22 To avoid identifying the humanitarian organisation or revealing the identities of our participants, we refer to any specific organisations mentioned as part of the case we report on as "international NGOs".

23 The humanitarian community decided during the early phases of the response not to rely on biometric verification. Human Rights Watch, "You Don't Need to Demand Sensitive Biometric Data to Give Aid. The Ukraine Response Shows How," 11 July 2023, https://www.hrw.org/news/2023/07/11/you-dont-need-demand-sensitive-biometric-data-give-aid-ukraine-response-shows-how.

for the promised funds?? It is very difficult for people without a penny in their pockets, and even when there are two small children who have no one, to leave and go to work! [...]" (anonymous social media user).

One participant who had worked on the response in question observed that, given Ukraine's tech-savvy population and an active media landscape, the humanitarian NGO found their services in high demand – a stark contrast to other humanitarian settings. They claimed: "We received tens of thousands, if not hundreds of thousands of responses within launching the programme immediately and I don't think we did a lot of advertising necessarily [...] in Sudan we instead have enumerators that go out and collect [...]" (KII participant 1). This emphasises the distinct nature of the Ukraine operation. Another study participant noted their impression that throughout the operation, consent was collected in a spur-of-the-moment way, in a box-ticking fashion rather than being taken seriously (KII participant 2).

Data Subject Requests for Deletion and Underlying Motivations

Following considerable delays with programme-rollout, the international NGO started receiving data subject requests for data deletion, including some explicitly citing GDPR as grounds for removal: "[W]e did receive a few GDPR removal requests, which was interesting. Not very many. I think in total there were [no] more than like 50 to 70 somewhere in that range" (KII participant 1). Framing the receipt of data deletion requests as a success in that it prompted organisations to revisit their practices and assumptions, a study participant stated that "it was a great moment when people in Ukraine asked some of our organisations to delete data because everyone freaked out and they realised [...] how much the data travels globally across all these organisations … it's like what the heck is it doing over there? It's [...] how our systems are set up. So then to delete it becomes a nightmare because you actually don't even know where it is" (KII participant 2).[24]

There was no immediate clear-cut explanation for these deletion requests which mentioned GDPR or were directed directly at the international NGO without explicitly referencing any DPL. Likely a combination of factors motivated the requests: First, dissatisfaction with humanitarian services, e.g. due to prolonged waiting times, played a role. One anonymous social media user called on fellow recipients publicly to "withdraw your data, submit to other organisations, there are many of them, the amount is the same for everyone"

24 The valuable reviewer feedback received for this submission prompted us to qualify this statement as an individual opinion. We stress that the data exchange systems put in place during the humanitarian response in Ukraine, including deduplication efforts, followed strict terms and conditions and that global transfers of data (even within organisations) are considered out of the ordinary.

(anonymous social media user). Since some humanitarian organisations were dispersing funds faster than others, this could have motivated the desire to switch providers of MPCA. This account is corroborated by our interview participants. Another social media user explicitly complained about being "locked-in" in the international NGO's system and not being able to receive funds from other organisations' CVA programmes: "I think people are more interested in the question of where their promised codes are, why you don't answer the questions posed to you in the [messenger] for three to five days, why people can't receive funds for the codes that you sent, since you made mistakes in the names of people in every second code sent, why people can't get funds in other [cash programmes], since you entered into the system the data […], but in fact no one received anything [...]" (anonymous social media user).

Second, having analysed the feedback forms for the humanitarian services provided, a study participant who had worked on the specific response in question found suggestions that recipients were concerned by the intrusiveness of the data collection: "We would have free text fields in some of our questions and sometimes people would just write 'why do you need to know this?' in those texts" (KII participant 1). One of the affected individuals venting their frustration on the public social media page of the international NGO explicitly referenced this, claiming that "the [international NGO] reportedly collected detailed information about every person who contacted it, including virtually all data (passport, […] registration address and real address, phone numbers, [etc.]). There are not even contacts of responsible persons who could clarify the situation." (anonymous social media user).

A third reason lies in the inherent risk profile of the data collected. Our humanitarian interlocutors expressed particular concern in this regard: "I think there were some genuine deletion requests for fear of … well, for fear of anything, right? Because we collected a lot of very sensitive information [...] like we had coordinates, we had disability status, we had like income and everything like it. It was really sensitive." They further specified that "[...] if this falls into the wrong hands, you basically have like a complete map with exact coordinates of where households are that are vulnerable [e.g.] that are headed by a single woman or whatever that have children in that or, you know, like [it's] really incredibly sensitive data. And so I think some of these households were reaching out to us for deletion requests on the basis that they don't want to have that risk" (KII participant 1). However, we were not able to directly verify from the collected social media data that the inherent risk profile motivated individual deletion requests.

A fourth final reason, they speculated, was that "gaming the system" by submitting concurrent applications to different aid providers to obtain illegitimate access to funds could also play a role in motivating data deletion and portability: "I really do believe that a majority of the people that sent

in the deletion requests were doing so out of concern for their own data privacy", but "[some individuals] submitted the self-registration form several times through different phones or they had people submittedsubmit for them or whatever, but they all routed back to the same bank ID or the same tax ID or whatever, so that the money would go to the same person essentially and I would suspect that some of these deletion requests might have been people trying to game the system" (KII participant 1). Due to a lack of evidence, we cannot pinpoint the assumptions motivating such requests, but they likely included an understanding of deduplication mechanisms and data sharing among humanitarian organisations. What this highlights is that the providers of aid themselves at times speculated about the exact motivations of affected individuals exercising their data subject rights, emphasising the need for further empirical research into how data handling practices are perceived in humanitarian settings.

Summary

In summary, we found that the CVA system design during the early humanitarian response following the full-scale Russian invasion of Ukraine exhibited risk factors in its reliance on external social media platforms and its tendency to collect sensitive personal data. Paired with delays in initial aid provision, this prompted negative reactions from the affected population, including data deletion requests. The speculative motivations for these requests included dissatisfaction with humanitarian services, the intrusiveness of the data collection, the inherent risk profile of the collected data, and attempts to illegitimately access funds.

We also found that responders were genuinely surprised by the strength of the reaction and the self-determination of the affected population. This contrasts with other humanitarian contexts and a sentiment echoed by an interviewed humanitarian worker from a different region with acute humanitarian needs: "A lot of the people in this space still look at them as beneficiaries and beneficiaries come with the expectation of silence, you receive and keep quiet" (KII participant 3). Observing and interpreting how the presence of DPL could empower recipients of aid opens important avenues for further research and learning in the humanitarian sector.

Conclusion and Outlook

Our objective in this chapter was to show how the presence of DPL and a rising awareness of data subject rights in affected populations are impacting the relationship between providers and recipients of aid by opening new accountability channels. To this end, we presented novel empirical evidence examining the motivations for data deletion requests based on a combination of

sources. Using a case study of CVA assistance in Ukraine, we developed four plausible motivations that prompted affected individuals to exercise their data subject rights under DPL. The high digital literacy of the affected population in Ukraine and the complementary (rather than replacement) role of humanitarian actors in providing social services there make this case an unusual but highly salient one that may foreshadow developments in other humanitarian contexts. As the humanitarian sector engages with affected populations that are increasingly digitally literate, connected, aware of, and empowered through DPL, the conventional relationship between providers and recipients of aid is changing.[25] More empirical evidence is needed in this area to fully understand the implications for humanitarian actors, and how they might differ between different types of organisations, especially as the normative influence of the GDPR is perceived even outside its direct geographic scope. The findings further highlight that through DPL, affected individuals could be responding directly to perceived humanitarian service quality, especially on CVA programmes with multiple providers, ultimately enforcing higher quality standards. However, it also opens up new potential risks, such as coordinated disinformation campaigns calling for data deletion requests against humanitarian actors that could seriously disrupt overall aid provision.

We sought to demonstrate, based on initial evidence, that the ideas behind DPL are permeating into the general consciousness among affected populations and can furnish individuals with the power to exercise limited control over the humanitarian actors providing aid. This can be considered a successful demonstration of the idea that data protection enables agency by providing an accessible accountability pathway to affected individuals. Our findings also raise important implications for future humanitarian contexts around the globe, where humanitarian organisations will have to navigate a complex and variegated landscape of overlapping DPL. One participant reflected on future changes across different geographies during the interview: "What I have noted in the past few years is that there's been a lot of data protection laws coming up in the different African countries" (KII participant 3). Another participant expanded on this in a hypothetical case in Somalia, highlighting that many aspects of future digital humanitarian action in contexts with DPL remain unclear: "So then you have this kind of dual mandate of two legislations that organise humanitarian organisations operating in Somalia [and they] need

25 The concepts of 'critical digital literacy' and 'techno-legal knowledge' offer promising starting points for a more systematic engagement with newly empowered 'beneficiaries'. Kristin Bergtora Sandvik, "Digital Refugee Lawyering: Risk, Legal Knowledge, and Accountability," *Refugee Survey Quarterly* 40, no. 4 (2021): 414–432, https://doi.org/10.1093/rsq/hdab013; Kristin Bergtora Sandvik and Kjersti Lohne, "The Struggle against Sexual Violence in Conflict: Investigating the Digital Turn," *International Review of the Red Cross* 102, no. 913 (2020): 95–115, https://doi.org/10.1017/S1816383121000060.

to comply with both of them [and] GDPR is much better sensitised. […] Organisations are aware of [GDPR] from their HQs down to the country. [...] Whereas the Somali legislation is much newer, it's not really enforced. So to my knowledge, there's been no cases of [it] being enacted, [but] there's the requirement to comply with the national legislation, especially where data is collected and stored." (KII participant 4).

To conclude, we have shown the value of empirical research into how DPL affects humanitarian contexts. We close this chapter by calling for further empirical research to provide a stronger evidence base for digital humanitarian action that is robust and effectively implements the data subject rights of affected populations and to highlight some areas for policy intervention. This should complement the long-standing, sector-wide engagement with DPL by providing data on the lived experience of data protection in humanitarian contexts. We encourage further sector-wide dialogue on how DPL affects the relationship between providers and recipients of humanitarian aid and developing an understanding of how the emerging fundamental changes to this relationship can upend the established processes of humanitarian action. Learning from salient cases, such as the early onset of humanitarian crisis response in Ukraine, allows the sector to prepare for humanitarian operations in other regions with rapidly increasing digital literacy and a complex DPL landscape, and retain its reputation as trusted, neutral, impartial, and independent providers of aid. Third, we advocate for the inclusion of DPL considerations in future scenario planning and preparedness exercises, respecting the likely fact that most humanitarian contexts will come with a complex local mix of perceptions around privacy, applicable DPL, and levels of digital literacy.

Ethics Statement

This research received ethics clearance from the University of Cambridge's Centre for Research in the Arts, Social Sciences and Humanities under the reference CRASSH REA 24/0001 in June 2024.

17

CONTEXT MATTERS

Towards a Framework for Understanding Perceptions of Data Protection in Humanitarian Aid

Timothy Charlton, Julia Feigen, and Silvia Pelucchi

Introduction

In the last century and a half of humanitarian action, organisations in this sector have repeatedly had to adapt their working modalities to new challenges, to remain able to deliver their services to some of the hardest hit areas of the world. In recent decades, among other things, this has entailed a progressive process of reflection on, and adoption of, digital tools and the new ways of working that they brought with them.[1] The reasons offered for this shift have been numerous: from improving efficiency and the delivery of services,[2] to adapting to the tools and expectations of the people targeted by humanitarian interventions[3] as well as of the donors who support specific initiatives.[4] In 2025, this process is still ongoing and is now confronting complex

1 See Chapter 1, "The Contribution of Data Protection to Humanitarian Action: Ten Years of Data Protection in Humanitarian Action".

2 This is particularly the case in discussions on innovation in humanitarian operations, starting from the 2009 Active Learning Network for Accountability and Performance (ALNAP) report on "Innovations in international humanitarian action", and discussed more explicitly in subsequent years. See IFRC, "World Disasters Report 2013: Focus on Technology and the Future of Humanitarian Action", Geneva (2013), https://www.ifrc.org/document/world-disasters-report-2013-focus-technology-and-future-humanitarian-action.

3 Patrick Meier, "New Information Technologies and Their Impact on the Humanitarian Sector," *International Review of the Red Cross* 93, no. 884 (2011): 1239–1263, https://doi.org/10.1017/S1816383112000318; International Committee of the Red Cross, The Engine Room, and Block Party, "Humanitarian Futures for Messaging Apps," January 2017, https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

4 A critical dissection of the role of communication technologies in the humanitarian sector responding to increased audit requests from donors can be found in: Mirca Madianou et al.,

DOI: 10.4324/9781003650164-24

evolutions in technologies that are simultaneously being hailed as a way to solve entrenched issues, and as an existential risk to the safety of people relying on humanitarian services.[5]

From their side, humanitarian organisations continue to proclaim their responsibility to follow the core humanitarian imperative of "do no harm" in all aspects of their operations, including innovation.[6] This entails the necessity to evaluate the adoption and deployment of new technologies with an eye to the expected benefits that these would bring, balanced against the very real costs (human, financial, and ethical) that they might engender. The reality on the ground, however, is much more complex. The last few years have seen numerous reports, analyses, and calls to action regarding the unintended, and often understudied, effects that the deployment of various "innovation" technologies, such as biometrics, artificial intelligence (AI), drones, or mobile cash, has brought into humanitarian spaces.[7] And while that complexity can hardly be reduced to a few causes and circumstances, one common thread frequently found at the basis of the tension is the amount of data that these

"The Appearance of Accountability: Communication Technologies and Power Asymmetries in Humanitarian Aid and Disaster Recovery," *Journal of Communication* 66, no. 6 (2016): 960–981, https://doi.org/10.1111/jcom.12258.

5 Artificial intelligence is arguably the most discussed example at the time of writing. See Ana Beduschi, "Employing AI to Improve Humanitarian Action in Times of Conflict and Crisis," *Research Handbook on Warfare and Artificial Intelligence* (Edward Elgar Publishing, 2024): 298–313, https://www.elgaronline.com/edcollchap/book/9781800377400/book-part-9781800377400-23.xml; Júlia Zomignani Barboza, Lina Jasmontaitė-Zaniewicz, and Laurence Diver, "Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection," *Privacy and Identity Management. Data for Better Living: AI and Privacy* (IFIP International Summer School on Privacy and Identity Management, Springer, Cham, 2020): 161–176, https://doi.org/10.1007/978-3-030-42504-3_11.

6 A good discussion on how the principle to "do no harm" is being articulated in humanitarian innovation can be found in: Jo Burton, "'Doing No Harm' in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action," *International Review of the Red Cross* 102, no. 913 (2020): 43–73, https://doi.org/10.1017/S1816383120000491.

7 Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and 'Big Data,'" *International Review of the Red Cross* 99, no. 904 (2017): 179–209, https://doi.org/10.1017/S1816383117000637; Irwin Loy, "Biometric Aid Data and the Taliban," *The New Humanitarian*, 2 September 2021, sec. Aid and Policy, https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban; "Updated – Thomson Reuters Selling US Immigration and Customs Enforcement (ICE) Access to Data," *Privacy International*, 28 June 2018, http://privacyinternational.org/long-read/2079/updated-thomson-reuters-selling-us-immigration-and-customs-enforcement-ice-access; Morgan Meaker, "Europe Is Using Smartphone Data as a Weapon to Deport Refugees," *Wired*, 2 July 2018, https://www.wired.com/story/europe-immigration-refugees-smartphone-metadata-deportations/; Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector," *Humanitarian Law & Policy Blog* (blog), 5 December 2016, https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/.

technologies are able to collect and who, ultimately, controls this data and the insights gained from it.[8]

In this perspective, data protection has frequently been identified as one of the frameworks at the disposal of humanitarian organisations to analyse and balance these risks. Beyond being a legal requirement under many jurisdictions and under regulatory frameworks of international organisations (IOs) with privileges and immunities, arguments in favour of more robust data protection practices in the sector have been made in operational and relational terms, especially with respect to an organisation's responsibility toward the people it aims to serve.[9] However, while a growing literature exists on the legal principles and implications of data protection frameworks in humanitarian action,[10] and, in parallel to it, a growing number of accounts document the concrete harms of privacy invasions and excessive surveillance in these spaces,[11] there still remains a significant gap. To date, there is limited scholarship on how the people targeted by humanitarian services experience this increased "datafication" of their relationship with humanitarian organisations, how much they resonate with the principles put in place, at least in theory, to better protect and empower them, and which factors are most likely to impact or influence this perception.[12] This is an important theoretical and practical gap, especially if these practices are implemented not just as a mandatory legal exercise, but as a way to ensure that people have better access

8 An early alarm bell on this was sounded in the 2013 Privacy International report "Aiding Surveillance". See Gus Hosein and Carly Nyst, "Aiding Surveillance," *Privacy International*, 1 November 2013, http://privacyinternational.org/report/841/aiding-surveillance.

9 Frequently, data protection is described as a manner to ensure that the dignity and rights of affected populations are respected by humanitarian organisations, as a way for humanitarian organisations to remain accountable to them under established standards, and as an extension of their duty to protect them from additional harm. This is further elaborated in the next section. See also e.g.: Delphine van Solinge and Massimo Marelli, "Q&A: Humanitarian Operations, the Spread of Harmful Information and Data Protection," *International Review of the Red Cross* 102, no. 913 (2020): 27–41, https://doi.org/10.1017/S1816383120000429.

10 Of which this publication is part, and to which several of its editors and authors have contributed elsewhere. See e.g.: Massimo Marelli, "The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders," *Computer Law & Security Review* 50, 1 September 2023, https://doi.org/10.1016/j.clsr.2023.105849; Massimo Marelli ed. ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition (Cambridge, 2024), https://doi.org/10.1017/9781009414630; Aaron Martin, "Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises," *Surveillance & Society* 21, no. 1 (2023): 96–102, https://doi.org/10.24908/ss.v21i1.16266.

11 See note 7 for examples and Chapter 16, "'Withdraw your data': How Data Protection Legislation can Reshape Humanitarian Action," for a critical reading of a more recent case.

12 Though there have been some attempts to remedy it in recent years, see "Balancing Aid and Privacy: Perceptions of Data Protection Policies for Cash Assistance in Ukraine," *Ground Truth Solutions*, September 2023, https://www.groundtruthsolutions.org/library/balancingaidandprivacy.

to their rights and are better protected from the increasing data processing activities of humanitarian organisations and other actors in this space.

The settings where humanitarian organisations operate and provide essential services are important sites for both academic and policy inquiry. Data collection and processing have become ubiquitous elements of humanitarian organisations' interactions with the persons and communities they serve. As such, it is imperative for humanitarian organisations to better understand and adapt to how the people targeted by their policies think about the use of their data and privacy, and what implications this has for the way an organisation interprets data protection principles and requirements and, consequently, processes personal data.

This chapter provides an initial contribution towards exploring this question. It is part of a broader collaborative study between the Data Protection Office (DPO) of the International Committee of the Red Cross (ICRC) and the Minderoo Centre for Technology & Democracy (MCTD) at the University of Cambridge.[13] The study seeks to understand how people affected by humanitarian crises understand, experience, and perceive the way humanitarian organisations process their data from collection to deletion. In so doing, it aims to address an empirical knowledge gap in a field concentrated on consumers' perceptions, where affected populations' perceptions remain understudied, and to develop a research agenda for future studies in this mission-critical area. This chapter reports on the preliminary ("pilot") phase of this study, which used expert interviews to develop an initial model of how such perceptions are structured, what assumptions are made by practitioners in this area, and what preliminary insights could be drawn from their experience regarding affected populations' perceptions.

Our point of departure is that perceptions are fundamentally shaped by individuals' contexts, and a preliminary categorisation of relevant environmental factors is a necessary first step in analysing how people react to humanitarian organisations' data processing activities. This, in turn, allows us to frame some preliminary considerations on relevant areas of intervention for humanitarian organisations aiming to analyse and manage those perceptions.

Over the following sections, we present findings on how humanitarian practitioners understand affected populations' perceptions of personal data collection by humanitarian actors. First, we familiarise the reader by mapping relevant assumptions. Then, we provide a high-level overview of perception research both generally and in humanitarian action and introduce the method and data collection strategy of this research. Finally, we present the findings

13 "The ICRC and CRASSH at the University of Cambridge to Launch New Humanitarian Action Programme," ICRC, 31 January 2023, https://www.icrc.org/en/document/icrc-and-crassh-university-cambridge-launch-new-humanitarian-action-programme.

of the research and conclude the chapter by discussing implications for the humanitarian sector and outlining a research agenda.

Assumptions about Data Protection in Humanitarian Action

Data protection in humanitarian action is designed around the core principle of "do no harm", developed through external legal requirements and internal policy frameworks, or individual data protection regulatory frameworks in the case of IOs, and applied through a variety of actions and practices.[14] There is no unified standard or code of conduct about data protection in humanitarian action,[15] and the applicability of Data Protection Legislation (DPL), such as the European Union's General Data Protection Regulation (GDPR) and national DPL, to humanitarian action[16] may differ based on whether organisations are non-governmental, subject to domestic laws, or IOs, with privileges and immunities to allow them to achieve their mandate under international law independently.[17] Despite the continuing evolution of data protection policies in humanitarian action,[18] some key assumptions can be identified (Table 17.1).

This initial "mapping of assumptions" around the relevance of humanitarian data protection practices was done between the cooperating organisations and was based on a structured conversation with four staff members at the ICRC DPO, and a workshop held between the ICRC DPO and MCTD in Cambridge in October 2024. The mapping process involved identifying the key objectives behind core data protection commitments and principles and articulating assumptions on their relevance for affected populations.

Broadly speaking, when discussing data protection in this sector, there seem to be three key and interconnected rationales underpinning it. The first is a logic of protection, which argues that by protecting often sensitive personal data necessary to conduct operations, humanitarian organisations are protecting the people to whom this data belongs. The second is a logic of accountability, which argues that people have specific internationally recognised rights

14 Marelli, ed., *Handbook on Data Protection in Humanitarian Action*.

15 Some humanitarian networks may adopt common guidelines, e.g. Tommaso Natoli, "The 33rd International Conference of the Red Cross and Red Crescent (2019)," *Yearbook of International Disaster Law Online 2*, no. 1 (2021): 383–392, https://doi.org/10.1163/26662531_00201_017.

16 Chapter 16, "'Withdraw your data': How Data Protection Legislation can Reshape Humanitarian Action".

17 Andrea Raab-Gray and Massimo Marelli, "Inviolability in the Digital Era: The ICRC's Agreement on Privileges and Immunities with Luxembourg," *International Review of the Red Cross*, 16 April 2025, 1–28, https://doi.org/10.1017/S1816383125000190.

18 Chapter 14, "Growing data protection maturity in humanitarian action: changes in the understanding of key concepts in theory and in practice".

TABLE 17.1 Mapping of principles and assumptions.

Principle	*Assumptions*		
	Protection	*Accountability*	*Trust*
Transparency and right to information To ensure data subjects know what is happening to their data and maintain control over it, humanitarian actors must communicate with affected populations about their data in a comprehensive and non-overwhelming way.	• Information about what happens to personal data makes it possible to express specific concerns about it.	• Lack of information about the processing of personal data disempowers affected individuals and creates anxiety.	• Affected individuals want to know what happens to their personal data.
Lawful and fair processing Personal data is processed according to explicit, transparent, lawful, and relevant rationales, which can be explained and justified. Lawfulness and fairness are critical to uphold agency and dignity, two cornerstones of humanitarian action. **Focus on: consent, as a traditionally preferred legal basis in humanitarian action** Consent ensures the individual is given full authority over what happens to their data. Valid consent must be uncoerced, fully informed, specific, and unambiguous. Despite humanitarian settings often being coercive, consent remains a prioritised option among available lawful bases for data processing.	• Affected individuals do not care what happens to their personal data or why it is processed, because they have more pressing concerns. • Affected individuals do not have the tools to understand the risks and benefits of processing their data through complex technologies, and too much information on it might just increase their distress.	• Affected individuals care about their personal data being processed only for legitimate reasons and feel empowered when this is clarified and confirmed. • Affected individuals feel empowered when making explicit choices about personal data.	• Affected individuals feel "forced" to give consent out of fear that otherwise they will not be able to obtain assistance and other services.
Purpose specification and data minimisation Personal data should be processed only for specific, legitimate, and explicit purposes with minimal privacy intrusion to achieve these purposes.	• In some instances, affected populations might share additional personal information in expectation of further services.	• Affected individuals prefer to provide only the minimum necessary personal information, and want to know why.	• Affected individuals might be made anxious when they are asked to provide personal details without clear objectives or reasons.

over their personal data, and humanitarian organisations have a responsibility to ensure they have the means to apply those rights when they are the ones processing their data. The third is a logic of trust, which argues that if people suffer, or perceive they have suffered, negative consequences because of the way humanitarian organisations process their data, they might lose trust in all the services provided and refuse such assistance, thus impeding them from accessing humanitarian relief and jeopardising the relationship between them and humanitarian organisations.

These three key rationales were then mapped onto key data protection principles and articulated as specific assumptions with respect to people's experience of them.

Perception Research in Humanitarian Action

Diversity and human nature lie at the centre of humanitarian action, meaning each humanitarian setting comes with unique constraints and context-specific requirements. Assessing and accounting for these local factors while maintaining a consistent level of service globally is a key challenge of international humanitarian organisations. Alongside institutional knowledge and experienced staff, obtaining an "inventory of needs from the perspective of affected populations" is central to tailored humanitarian responses.[19] Therefore, the perceptions of affected populations are widely monitored by humanitarian actors using qualitative and quantitative instruments to adjust their services to the needs of affected populations, mitigate hostile perceptions,[20] and improve their performance,[21] commonly referred to in the sector as *perception studies.*

Today, a large proportion of humanitarian action is intermediated by digital technologies[22] and increasing amounts of personal data are collected during humanitarian programmes in unfolding and protracted emergency or conflict situations. In 2022, over 21% of global aid was assumed to be delivered

19 Karin Hugelius, "Measurement of Perceived Needs in Humanitarian Contexts Using the HESPER Scale: A Scoping Study with Reflections on the Collaboration between Researchers and Humanitarian Actors," *Conflict and Health* 16, no. 1 (2022): 44, https://doi.org/10.1186/s13031-022-00478-6.

20 Hugo Slim, "How We Look: Hostile Perceptions of Humanitarian Action," Conference on Humanitarian Coordination, Wilton Park Montreux: Centre for Humanitarian Dialogue, 2004, https://gisf.ngo/wp-content/uploads/2014/09/0211-Slim-2004-How-we-look.pdf.

21 Elysée Nouvet et al., "Opportunities, Limits and Challenges of Perceptions Studies for Humanitarian Contexts," *Canadian Journal of Development Studies / Revue Canadienne d'études du Développement* 37, no. 3 (2016): 358–377, https://doi.org/10.1080/02255189.2015.1120659.

22 Catarina Mauritti Granjo, "Humanitarian Action and the Digital Age," CISE E-Working Papers (Lisbon, Portugal: CIES, 2021), https://cies.iscte-iul.pt/np4EN/3073.html.

through cash or voucher assistance[23] and today's rate is likely significantly higher. The biometric identity management systems set up to reduce duplication of registered recipients push humanitarian actors to extract increasing amounts of highly sensitive data from populations affected by disaster or conflict.[24] At the same time, sophisticated cyberattacks against humanitarian organisations reveal the true value of such data and the risks and safety concerns associated with appropriately collecting, storing, and sharing it.[25] There is a knowledge gap around how data-intensive humanitarian interventions and the data protection measures that accompany them are perceived by affected populations. To address it, we turn to the published literature to assess how perceptions on technology are measured in the general population and what methods underpin specifically humanitarian perception studies.

Understanding perceptions is central to humanitarian operational decision-making. For example, the (mis)perception of humanitarian drones as military equipment by the population[26] could jeopardise the delivery of aid, damage the reputation of humanitarian actors, or induce harm within the population itself. The same applies to other 'dual use' technologies.[27] Understanding the technological preferences of affected populations could allow humanitarian actors to tailor their responses to the local context, improving access and ultimately leading to more efficient use of funds.

To situate our pilot study in the wider literature on both technology-related and humanitarian perception research, we conducted a limited literature review. We paid particular attention to the methods and sampling strategies used in previous perception studies.

General Perceptions of Technology and Privacy Concerns

Studies of whether science and technology have a positive impact on society, such as a 2013 survey of member countries of the Organisation for Economic

23 "The State of the World's Cash 2023. Chapter 2: CVA Volume and Growth," The CALP Network, accessed 10 May 2025, https://www.calpnetwork.org/web-read/the-state-of-the-worlds-cash-2023-chapter-2-cva-volume-and-growth/.

24 Hayes, "Migration and Data Protection," 179–209; Chapter 4, "The logic of biometrics and organisational accountability".

25 Kristin Bergtora Sandvik, "The Centralization of Vulnerability in Humanitarian Cyberspace: The ICRC hack revisited," *Humanitarian Extractivism*, 2023, https://doi.org/10.7765/9781526165831.00008.

26 Joe Belliveau, "Humanitarian Access and Technology: Opportunities and Applications," *Procedia Engineering* 159 (2016): 300–306, https://doi.org/10.1016/j.proeng.2016.08.182.

27 Almudena Azcárate Ortega, "Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems," *Lawfare*, 6 May 2023, https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems.

Co-operation and Development (OECD), suggest that a majority of individuals take a favourable stance on the issue.[28] A large-scale survey of European Union (EU) member countries[29] also demonstrated a generally positive attitude towards science and technology from the majority of participants across the sample (77%). A 2016 study using experimental methods further bolsters the notion that technology itself might be associated with trust and confidence in the general population. Using simulated investment decisions, the authors found a "'technology effect' bias in decision-making".[30] This research references previous ethnographic studies demonstrating how technology moderates the quality of social relationships by shifting expectations of trust away from human counterparts.[31] Further, a literature-based study elaborates how the socially constructed novelty and usefulness of technological innovation are embodied in technologies' outer form and how it is perceived.[32]

Privacy concerns among users of digital technologies are a specific subset of perception research. Studies in the health sector, which offer relevant parallels to the humanitarian sector, have assessed the willingness of people to provide data for a perceived "public good",[33] drawing on the psychological Elaboration Likelihood Model (ELM), a conceptual lens to assess attitude and persuasion, and the Concern for Information Privacy (CFIP) scale instrument.[34] A modernised version of the CFIP instrument, the "Internet users'

28 OECD, "Public Perceptions of Science and Technology," *OECD Science, Technology and Industry Scoreboard 2015: Innovation for Growth and Society* (Paris: OECD Publishing, 2015): 234–247.

29 European Commission, "Responsible Research and Innovation (RRI), Science and Technology," *Special Eurobarometer* (Brussels, Belgium: Directorate-General for Research and Innovation, 2013).

30 Brent B. Clark, Christopher Robert, and Stephen A. Hampton, "The Technology Effect: How Perceptions of Technology Drive Excessive Optimism," *Journal of Business and Psychology* 31, no. 1 (2016): 87–102, https://doi.org/10.1007/s10869-015-9399-4.

31 Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other*, Third edition, revised trade paperback edition (New York: Basic Books, 2017).

32 Violina P. Rindova and Antoaneta P. Petkova, "When Is a New Thing a Good Thing? Technological Change, Product Form Design, and Perceptions of Value for Product Innovations," *Organization Science* 18, no. 2 (2007): 217–232, https://doi.org/10.1287/orsc.1060.0233.

33 Corey M. Angst, "Protect My Privacy or Support the Common-Good? Ethical Questions About Electronic Health Information Exchanges," *Journal of Business Ethics* 90, no. 2 (2009): 169–178, https://doi.org/10.1007/s10551-010-0385-5; Angst and Ritu Agarwal, "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion," *MIS Quarterly* 33, no. 2 (2009): 339, https://doi.org/10.2307/20650295.

34 H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* 20, no. 2 (1996): 167, https://doi.org/10.2307/249477.

information privacy concerns" (IUIPC), was tailored specifically to digital settings.[35]

Single question assessments of individuals' privacy concerns, while less methodologically rigorous, offer low barriers to deployment that could be critical in humanitarian contexts. Another alternative to full psychometric survey-based measurement in perception research is to provide anchors to participants by elaborating certain scenarios or *vignettes*, and then proceeding with a set of scales based on the literature, which offers an interesting middle-ground between psychometric and context-informed approaches.[36] Experiments further build on this idea by setting explicit contexts.[37] Context, i.e. the interplay of various factors, including location, timing, local setting, etc., is emerging as a central area of privacy research.[38]

Another method of assessing privacy concerns is to rely on observational methods and identify indicators of *revealed preferences*. For example, this could take the form of specific technical or social avoidance tactics, e.g. using a virtual private network (VPN) to hide one's online identity or, in a humanitarian setting, using multiple mobile phones or deliberately providing false information during registration. Further evidence for observational methods is provided by an early study which suggests that surveys of users' privacy concerns yield sub-optimal results when they are not conducted within the same context and that observational techniques are more likely to yield high-quality data.[39]

In summary, while a full deployment of psychometric survey instruments is commonplace in perceptions research, various adaptations exist to accommodate for complex settings based on contextual factors. These could be of interest to humanitarian settings, where research is often severely constrained by the availability and reachability of participants, conflicting interests, and safety concerns.

35 Naresh K. Malhotra, Sung S. Kim, and James Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* 15, no. 4 (2004): 336–355, https://doi.org/10.1287/isre.1040.0032.

36 An example is the survey on "Privacy and Identity Management for Europe" (PRIME) cited in Preibusch (2013). The full survey instrument is currently unavailable online (19 June 2025).

37 Sören Preibusch, "Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments," *International Journal of Human-Computer Studies* 71, no. 12 (2013): 1133–1143, https://doi.org/10.1016/j.ijhcs.2013.09.002.

38 Tawfiq Alashoor, "The General Relativity of Privacy," *ECIS 2024 TREOS*, 2024, https://aisel.aisnet.org/treos_ecis2024/30.

39 Kay Connelly, Ashraf Khalil, and Yong Liu, "Do I Do What I Say?: Observed Versus Stated Privacy Preferences," *Human-Computer Interaction – INTERACT 2007* 4462, ed. Cécilia Baranauskas et al., Lecture Notes in Computer Science (Springer Berlin Heidelberg, 2007): 620–623, https://doi.org/10.1007/978-3-540-74796-3_61.

Humanitarian Perception Research

Humanitarian perception studies generally address one or multiple of three core areas: a) aid gaps,[40] i.e. perceptions around the quality of aid provided, b) an inventory of needs,[41] i.e. perceptions around whether aid reaches the appropriate populations and c) hostility,[42] i.e. adverse perceptions or lack of trust in specific populations. Recently, questions around how data protection is perceived in the context of cash-based humanitarian assistance have been included in quantitative humanitarian perception studies.[43] The studies we reviewed relied on a variety of methods, with few studies reporting results from systematic large-scale surveys. One popular survey instrument is that developed by the World Health Organization (WHO), "Humanitarian Emergency Settings Perceived Needs Scale" (HESPER). It was designed to "provid[e] a quick and scientific method of assessing the perceived needs of people affected by large-scale humanitarian emergencies, such as war, conflict or major natural disaster".[44] Scale items were generated based on 14 previous methodologically diverse studies[45] in multiple geographic regions in Asia, Africa, the Middle East, and Central America. A dedicated web-version of this instrument (HESPER-web) has also been proposed.[46] However, a recent scoping study of HESPER and HESPER-web usage emphasises the need for a robust sampling strategy to gain valid insights from humanitarian settings, which can be a financial and logistical obstacle in volatile humanitarian situations.[47]

One multi-country telephone survey of multiple humanitarian contexts relied on expectation-confirmation theory to prime participants on four themes: participation, information, transparency, and aid relevance by asking

40 Greg Hansen, "The Ethos–Practice Gap: Perceptions of Humanitarianism in Iraq," *International Review of the Red Cross* 90, no. 869 (March 2008): 119–136, https://doi.org/10.1017/S1816383108000076.

41 Desiree Bliss and Jennifer Campbell, "The Immediate Response to the Java Tsunami: Perceptions of the Affected," (Fritz Institute, 2007); Hugelius, "Measurement of Perceived Needs".

42 Slim, "How We Look".

43 Serhii Tyutik, "Balancing Aid and Privacy: Perceptions of Data Protection Policies for Cash Assistance in Ukraine," *Ground Truth Solutions* (2023), https://www.groundtruthsolutions.org/library/balancingaidandprivacy.

44 WHO, "The Humanitarian Emergency Settings Perceived Needs Scale (HESPER): Manual with Scale," 2011, 94.

45 Among the evaluated methods were (semi-)structured interviews, household panel surveys, focus groups, and key informant interviews.

46 K. Hugelius, M. Semrau, and M. Holmefur, "HESPER Web – Development and Reliability Evaluation of a Web-Based Version of the Humanitarian Emergency Settings Perceived Needs Scale," *BMC Public Health* 20, no. 1 (2020): 323, https://doi.org/10.1186/s12889-020-8387-4.

47 Hugelius, "Measurement of Perceived Needs".

about their expectations, and subsequently probing them on their actual experience, highlighting the usefulness of a context-aware research design.[48]

When researching perceptions related to privacy concerns or technology using surveys, it is generally appropriate to rely on existing measurement instruments where available and adapt them to a specific context.[49] To gather the relevant background information for a study specifically related to the perceptions and experiences of humanitarian data processing, we conducted a pilot study with expert practitioners in Kenya, a country directly and indirectly (through neighbouring countries) exposed to humanitarian situations. We interpreted the situations described by the study's participants both directly and in terms of the *revealed preferences* of the affected populations to which the participant was exposed to through their humanitarian practice.

This chapter contributes the findings from this pilot study to the available perception studies literature by providing contextual details from the perspective of experts and humanitarian practitioners on the factors shaping recipients' perceptions. It seeks to address the intersection of assumptions made by humanitarian actors around the role and purposes of data protection guarantees, and the perceptions of affected populations about technology and data handling by asking the following research questions:

1. How are affected individuals' perceptions of digital technologies and the processing of personal data in humanitarian settings shaped?
2. How do the assumptions made about the relevance of personal data protection by humanitarian actors align with affected populations' perceptions and concerns?

Research Design and Methods

In this section, we draw primarily on key informant interviews (KIIs) conducted in a field setting (Kenya) chosen for its proximity to "data-intensive" humanitarian programmes and easy access to a diverse group of stakeholders. Interviews were conducted by two researchers during July and August 2024. KIIs are qualitative interviews with a wide range of participants from a community who have first-hand expertise in a certain topic area. During the interviews, participants were requested to recount "critical incidents", i.e. situations involving digital technologies which, in their opinion, illustrated how perceptions of technology and data processing were formed in humanitarian settings. These were treated as *vignettes* and discussed with other participants.

48 Ground Truth Solutions, "Listening Is Not Enough," Global Analysis Report (Geneva: OCHA, 2022).

49 Preibusch, "Guide to Measuring Privacy Concern".

Depending on capacity, interviews were conducted with one or two researchers and one or two participants. Where possible, interviews were conducted in-person, recorded, and transcribed. In some cases, virtual interviews were held, and field notes were taken. The research received ethics clearance prior to commencing.[50]

Data Collection

In the context of this study, we focused on two partially overlapping communities, 1) experts in the data protection domain, particularly those with experience of its applicability to humanitarian action, and 2) front-line humanitarian practitioners who deploy "data-intensive" services to affected populations. Initial interviews were used to generate leads to further participants. We conducted 17 semi-structured interviews with a total of 26 participants from local humanitarian organisations, IOs and NGOs, government entities, and civil society organisations (Table 17.2).[51]

Findings

Analysing the interviews produced three types of relevant findings. First, participants relayed a range of perceptions as part of their first-hand experience and interactions with affected populations. Second, it revealed contextual

TABLE 17.2 Organisational Affiliations of Key Informants

Type	*Participants*
International organisation (IO)	P-07, P-08, P-14, P-15, P-25, P-26
International NGO	P-03, P-04
Local humanitarian organisation	P-05, P-06, P-10, P-13, P-18, P-19, P-20, P-21
Funding body	P-16, P-17, P-23, P-24
Civil-rights organisation	P-01, P-02, P-09, P-22
Government body	P-11, P-12

50 Ethics clearance was granted by the Centre for Research in the Arts, Social Sciences and Humanities (CRASSH) at the University of Cambridge (CRASSH-REA 24-0001) and the Ethics Review Board at the ICRC (EERN 1524).

51 Where permission was obtained, interviews were recorded and transcribed. Transcripts were uploaded into the Atlas.ti web-based qualitative data analysis (QDA) environment and coded collaboratively using descriptive coding. Afterwards, emergent codes were clustered into salient themes representing the key factors influencing perceptions of technology and the processing of personal information in humanitarian settings.

factors affecting the way perceptions of technology use and the core assumptions of data protection are formed in humanitarian settings. Third, participants in the initial "pilot" phase shared various key events that exerted an influence on public perceptions, such as outrage over the misappropriation of photographic material, rumours about internet slowdowns, and emergency broadcasts misattributed to illicit data sharing between public and private institutions. In the following section, emergent *codes* and *themes* are presented in italics.

Perceptions of Affected Populations from the Perspective of Expert Practitioners

The first theme included an understanding that commonly practised biometric verification can be contentious among populations (P01; P02), a strong assumption that data collection (and providing personal data) would lead to receiving humanitarian assistance (P04; P05; P06; P14; P15), increasing fatigue among over-assessed populations (P14; P15), adverse reactions to joining large humanitarian programmes rather than local *ad hoc* efforts (P10), and distrust of humanitarian actors' technologies, particularly those of the UN (P14; P15).

Contextual Factors Affecting Perceptions

Beyond the *critical humanitarian needs* of an affected population, the contextual factors can be assigned to three categories: *group factors*, *individual factors*, and *the timing of historical events*.

Group Factors. One of the key emergent factors at the group level concerned the level of *awareness* of data protection standards, regulation and legislation in the population as well as the visibility of means of contacting the authorities on such matters. The presence of dedicated awareness-raising campaigns, either by the authorities or humanitarian actors, was emphasised as making a difference, and while the overall level of awareness was increasing, laws and regulation often outpaced understanding among the population (P07; P08). One participant mentioned that affected populations in the region of their operations were not aware of the cross-border nature of data transfers "to the level that everyone else might be aware of [it]" (P03).

Institutional trust, both in private and public sector institutions as well as technology itself, emerged as a factor during the qualitative analysis. Operating under a "trust deficit between the people and the government" (P-22) can negatively impact perceptions of the independence of humanitarian agencies or data protection regulators (P-09), especially where entanglements between the government and the private sector (e.g. mobile network operators) feature in the media. One participant explicitly referred to reactions among affected

populations in countries in the region (i.e. Kenya, Somalia, and Ethiopia) caused by perceptions of data mishandling in relation to government entities, leading to decreased levels of assistance: "They don't want to share, don't want to provide their data if they know that these data are going to be shared with the government authorities" (P16; P17). Private multinational tech companies were also implicated in deficiencies (P22). On the other hand, technology itself can play a different role by either increasing or decreasing trust depending on which context it is deployed in. One participant mentioned that affected individuals "attach a certain level of importance to electronic tools [rather than e.g.] notebooks" (P-03). This suggests that other contextual factors, e.g. locality, previous exposure to technology, and prevailing narratives or media coverage, determine whether digital solutions function as trust-enhancing or trust-inhibiting factors. The danger, as one participant elaborated, is that public opinion on technology is increasingly volatile and subject to mis/dis-information or rumours with the potential to impact humanitarian operations: "Even if there is really no evidence […] as long as [people] talk about it, it becomes like a perception, and then people start, you know, adjusting based on this" (P14; P15). Finally, participants referred to specific instances where trust in humanitarian actors was affected by cases of data mishandling or breaches of confidentiality (P01; P02). Misappropriation of photographic imagery played a central role here and serves as a tangible and recognisable example within the general population brought up by multiple participants.

The *cultural context* in which humanitarian technology is deployed was reported as having a significant effect on how perceptions on technology use and privacy are formed. This included the presence of *community elders or leaders* who often serve as gateways for humanitarian organisations and who may provide lists of vulnerable individuals (P14; P15) and exercise significant influence over perceptions among a group. At a higher level, there might be differences in factional control within a region (e.g. Somalia) which could impact technological preferences or concerns, e.g. related to which mobile carrier to use. Anecdotal evidence from one participant suggests that certain individuals in volatile regions adopt technological adaptation strategies, such as carrying multiple SIMs or devices to separate their interactions, e.g. with humanitarian agencies or government entities (P14; P15). In complex regions with an often diverse multi-ethnic or tribal population, granular regional differences in perceptions of technology use can emerge from predispositions held, e.g. against having photographs taken (P03).

Individual Factors. This category covers numerous intra-individual factors that relate to the individual's life course[52] rather than shared customs or

52 Janet Zollinger Giele and Glen H. Elder, eds., *Methods of Life Course Research: Qualitative and Quantitative Approaches* (Thousand Oaks: Sage Publications, 1998).

beliefs. Among the factors identified by the interview participants were *formal education* and *language use*, with one participant suggesting they were "not 100% sure that [affected individuals] understand the [definitions and terms] as we do based on […] their level of education" (P07; P08). This relates to a (lack of) awareness about the long-term repercussions or cross-border and cross-institutional sharing of data hidden behind bureaucratic 'taken-for-granted' terminology. Beyond access to formal education, participants suggested that membership of a *generational cohort*, e.g. being born in a period when smartphones were readily available as a member of "Gen Z", could be a determining factor itself, with a propensity among younger cohorts to question why a certain piece of information might be needed.

Geographic factors alone are not sufficient to explain perceptions which differ substantially along tribal or cultural lines per group and vary individually based on levels of *education*, *age* and *familiarity with certain technologies* (P04). Despite this, an *urban-rural divide* was raised as an important factor, though participants acknowledge that this could stem from the availability and affordability of technologies, such as smart or feature phones, and a subsequent lack of *tech-savviness* (P14; P15). According to one participant, the reliance of humanitarian actors on mobile *connectivity* (P03) can sometimes lead to the exclusion of populations: "we are trying to get you, [if] you're not connected, you're not near where there's network, you don't get […] assistance" (P07; P08). Participants' reporting about incidents in the Kenyan context singled out the capital region of Nairobi as an area of sensitivity and caution regarding the disclosure of personal information and data handling (P01; P02; P13).

Timing. A heightened sensitivity towards issues of data protection might permanently or temporarily be the result of the *timing* of major events, such as an election (P14; P15) that sensitises individuals, prompts additional *media attention* or *rumours*, and affects the overall *security situation*.

Critical Incidents

Our conversations with experts repeatedly returned to certain key events that strongly influenced perceptions around data handling. The first event concerned perceptions of data mishandling following a message broadcast by humanitarian actors in the wake of a flooding emergency. Increasingly, questions were raised about data sharing between humanitarian actors and the private companies operating mobile phone networks, leading to a sense of privacy infringement. It is worth noting that, as far as we were able to discern, messages were broadcast based on geographical criteria using mobile network cells rather than being individually targeted.

The second event involved anecdotal evidence of irregular data sharing between government entities and financial service providers following

a disaster response in a rural area of Northern Kenya. Again, we were not able to independently verify the underlying event beyond its featuring in the local public discourse around data protection as perceived by the interviewed experts and practitioners.

The third salient incident described by the participants of the pilot study concerned the misappropriation of personal photographic data. Specifically, respondents reported receiving pushback from affected individuals citing cases of photographs used in communication campaigns of humanitarian actors without explicit consent.

The fourth salient incident was related to the anti-government protests in Kenya during 2024. Interview participants reported a growing distrust in the population due to the perceived weaponisation of mobile communications infrastructure, such as the slowdown of internet connectivity around critical demonstrations to inhibit communications between protestors and media access.

Discussion and Future Research

The interviews revealed a series of factors that the interviewed experts and providers of humanitarian assistance thought to be central to the formation of perceptions of data handling among aid recipients. This inventory of factors forms the beginning of an empirical answer to the first research question. We found that perceptions around technology use and data processing varied considerably and we were able to identify four overarching groups of factors affecting perceptions: *group-level factors*, such as the level of trust in private and public institutions in a region; *individual-level factors*, such as the level of formal education attained or membership in a generational cohort that grew up with connectivity; the *severity of the humanitarian needs*; and the *timing of historical events*, such as protests or elections that might heighten sensitivity to data protection concerns.

We recommend future research consider this "context-aware" model when designing data collection strategies, drawing on the developed model for a robust theoretically-informed sampling strategy, a major hurdle to effective humanitarian perception studies identified in the literature. Since collecting a representative or systematic sample is highly resource-intensive, identifying individuals based on the stated criteria to avoid oversampling a specific opinion and enable comparative analysis will further enhance our understanding of perceptions in this critical field.

As per the second research question, which opens inquiry into the assumptions humanitarian actors make regarding affected individuals' perceptions, the factors we identified also reveal underlying resonance with the rationale for data protection principles. Through analysing input from our respondents,

there are three key themes that come to the fore: *transparency*, *purpose limitation*, and *informed consent*.

The principle of *transparency* underpinned many of the insights we collected, particularly when practitioners relayed concerns relating to the mishandling of personal information. Specifically, the interview participants expressed their impression that people were not always aware *who* had access to their data once it was collected, and that some feared it was passed along improperly to non-humanitarian actors. Some explained that it was this sense of not knowing that bred mistrust of, or even resistance to, data collection by humanitarian actors. Such concerns over third-party access to sensitive information, or the repurposing of data for reasons other than those initially provided, can be interpreted as revealing an expectation of transparency among affected populations. The expert interviewees of this pilot study generally assumed that affected individuals expect the handlers of their personal data (including humanitarian actors) to abide by clear standards for data collection and processing. Without this transparency, as suggested by respondents, humanitarian organisations risk exacerbating mistrust in humanitarian data handling. From an operational standpoint, trust looms large as an enabling factor of humanitarian action.[53] The link we observed between transparency and trust therefore signals that transparency, particularly in the context of data collection and processing, may possess significant operational value to humanitarian actors.

In citing critical contentious events, such as organised protests and elections, individuals highlighted another source of mistrust. Differing from the mistrust targeted towards third-party data processors, it relates to threats from technology itself. For example, during the 2024 anti-government protests in Kenya, some attributed poorly functioning internet and blocked communication channels between protestors to purposeful manipulation of telecommunications infrastructure technology. This notion that technology can be intentionally compromised to serve ulterior interests spoke to concerns that the purpose for which technology is designed is not necessarily the purpose for which it is ultimately used.

Like infrastructure technologies, data can also be multipurpose.[54] Also known as "function creep",[55] the capacity of data to be shared and used for different purposes in the future renders it a potent source of concern. The sense of anxiety that permeated comments on the misappropriation of technology

53 ICRC, "Principled Humanitarian Action Relies on Trust," 16 December 2019, https://www.icrc.org/en/document/principled-humanitarian-action-relies-trust-0.

54 Aaron Martin and Linnet Taylor, "Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice," *Information Technology for Development* 27, no. 1 (2021): 51, https://doi.org/10.1080/02681102.2020.1811943.

55 Martin and Taylor, "Exclusion and Inclusion in Identification," 65.

during critical events suggests general distrust of technological function also among humanitarian actors. Such sentiments directly tie into the data protection principle of *purpose limitation*. The concept of purpose limitation, which instructs data handlers to "determine and set out the specific purpose(s) for which data are processed"[56] embodies the expectation that the handler does not use the data beyond its stated purpose. Based on these preliminary discussions, this is in line with the interests of affected people, and transparency on this aspect could help reinforce trust.

Finally, the question of *informed consent* came up as a prominent concern among participants. Specifically, the issue of photography without consent was mentioned repeatedly, and humanitarian professionals noted the sense of violation individuals felt when they were photographed without permission. In some instances, individuals stated that people were unaware they were being photographed by humanitarian organisations and only learned once they saw themselves featured in institutional promotional material. Preventing such feelings of violation, whether they originate from unwanted photography or extractive information gathering, underpins the purpose of informed consent both from a relational perspective centred on trust, and from an accountability perspective.[57]

Limitations and Recommendations for Future Research

This chapter provides initial empirical evidence from the perspective of domain experts and providers of humanitarian aid on the key factors shaping how individuals affected by humanitarian situations perceive the increasing use of digital technologies by the providers of humanitarian aid and the assumptions underpinning their data protection efforts. However, the sensitive nature and ethical considerations limited the research methods during the exploratory "pilot" phase. First, we were geographically limited to one region, the Nairobi capital region in Kenya. We chose this location due to its accessibility and its proximity to various acute humanitarian crises. Second, we did not directly approach affected populations but chose instead to engage with experts who are knowledgeable about digital technology use and exposed to affected populations. Limited access to affected persons influenced the choice to interview humanitarian practitioners. While this group of experts provided helpful insights and relevant context, the findings derived from their contributions mark the beginning, rather than the end, of exploration on this topic.

56 Marelli ed., *Handbook on Data Protection in Humanitarian Action*, 22.

57 Madeleine Maxwell, "Unpacking 'Informed Consent'," *The Engine Room* (blog), 2019, https://www.theengineroom.org/library/unpacking-informed-consent/.

Ultimately, the insights we gathered are narratives of affected individuals' perceptions by those working closely with them through humanitarian operations. It is necessary to acknowledge that these impressions reflect the experiences and biases of the speaker. These contributions should therefore not be considered substitutes for hearing from people directly. However, they mark an important reference point for future investigation. Reflecting on how practitioners perceive the experiences of the communities they serve sheds new light on how the humanitarian sector approaches and understands the processing of personal information. Their opinions are highly relevant to the evaluation of data protection practices and can influence data protection policy over time.

Given this initial inquiry, we suggest that future research should expand the scope to directly sample affected populations and diversify the geographic and operational settings. However, we urge researchers to consider the harms that such practices can create. As has been well-documented in critical literature, the phenomenon of "over researched" refugee populations in East Africa, particularly in Kenya, is a growing risk.[58] Given that refugee populations are often recipients of humanitarian assistance and targeted programming, the concern regarding their over-exposure to researchers was appropriate in this context to avoid "research fatigue" among refugees who experience frequent requests for participation from researchers.[59]

The cost of over-researching some groups does not simply amount to growing frustration among research participants, but it can cause psychological harm, often referred to as "retraumatization".[60] It is therefore our strong recommendation that future research in this area seeks to widen the scope of its participants to learn directly from affected people in a way that is respectful of their past and current circumstances. As researchers working alongside the humanitarian sector, we similarly aim to "do no harm" in our own work. The methods and decisions we chose for this study reflect that imperative.

58 Naohiko Omata, ""Over-Researched" and "Under-Researched" Refugee Groups: Exploring the Phenomena, Causes and Consequences," *Journal of Human Rights Practice* 12, no. 3 (2020): 681–695, https://doi.org/10.1093/jhuman/huaa049.

59 Omata, ""Over-Researched" and "Under-Researched" Refugee Groups," 682.

60 Amanda Weiss, "Beyond Retraumatization: Trauma-Informed Political Science Research," (OSF, 2022), 4, https://doi.org/10.31219/osf.io/rvksp.

18

DATA PROTECTION AND THE ASIA-PACIFIC REGION

Zooming into Humanitarian Action

Hiroshi Miyashita

Introduction

The United Nations (UN) lists 53 countries in Asia-Pacific with approximately 4.7 billion people, or 60 per cent of the world's population as of 2023.[1] The diverse cultures, languages, religions, and traditions have made for varying approaches to protecting privacy and personal data.

While there is no single human rights organisation in Asia-Pacific, the existing privacy frameworks are the APEC (Asia-Pacific Economic Cooperation) Privacy Framework of 2005 and the ASEAN (Association of Southeast Asian Nations) Framework on Personal Data Protection of 2016. The Brussels Effect, which refers to an external effect on third countries through the European Union's (EU) regulatory frameworks,[2] impacts Asian jurisdictions as the GDPR (Regulation (EU) 2016/679) provides the cornerstone of each jurisdiction's data protection law.[3] The EU's influence can also be illustrated by the EU's adequacy decisions on Japan and South Korea, together with the convergence of the ASEAN framework and EU Standard Contractual Clauses. Furthermore, cross-border e-commerce and trade relationships create commercial pressure that incentivises Asia-Pacific countries

1 United Nations Economic and Social Commission for Asia and the Pacific (UN ESCAP), *Asia-Pacific Population and Development Report 2023* (2023): 2, https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/undesa_pd_2024_escap-report-population-development-17.pdf.

2 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).

3 Ching Him Ho and Anselmo Reyes, "Introduction," *Privacy and Personal Data Protection Law in Asia*, ed. Adrian Mak et al. (Hart Publishing, 2025): 4.

DOI: 10.4324/9781003650164-25

to establish or strengthen data protection laws in order to build trust with trading partners and consumers.[4]

However, it is important to note that not all the Asian constitutional models reflect European values such as human rights, democracy, and the rule of law. Instead, some models of non-liberal constitutionalism in Asia are rooted in religious, socialist, or communitarian values.[5] Notwithstanding these differing frameworks, several Asian approaches to humanitarian activities have illustrated how community empowerment can occur even within alternative constitutional orders. Apart from the traditional Western humanitarian order, non-Western governments and organisations are becoming increasingly important and visible contributors to international humanitarian assistance in Asia-Pacific.[6] The origin of Eastern philanthropy is rooted in its traditional norms or beliefs. A Chinese Confucian philosopher, Mencius, marked 'benevolence' as 'human-heartedness, goodness, love, altruism and humanity'.[7] Buddhism, despite its diverse forms, is understood as 'many consecutive lives of piety and charity'[8] in India. The soul of the Samurai in traditional Japanese society also reflected the humanity of rescuing the injured, so, as Inazo Nitobe noted in the early 1900s, 'the Red Cross movement, considered peculiarly Christian, so readily found a firm footing among us'.[9] Although there is no single unified concept of humanity in the Asia-Pacific region, humanitarian activities have become more coordinated following a series of natural disasters.

This chapter does not analyse the whole Asia-Pacific region, rather, through a literature review, it explores shared privacy and data protection challenges that arise in the context of humanitarian activities. The following section provides case studies on privacy and data protection in natural disasters and social media across the Asia-Pacific region, highlighting the importance of careful compliance with data protection laws to prevent what might be termed

4 Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford University Press, 2014): 558; Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992): 222.

5 Li-ann Thio, "Varieties of Constitutionalism in Asia," *Asian Journal of Comparative Law* 16, no. 2 (2021): 285, https://doi.org/10.1017/asjcl.2021.23.

6 Jacinta O'Hagan and Miwa Hirono, "Fragmentation of the International Humanitarian Order? Understanding 'Cultures of Humanitarianism' East Asia," *Ethics & International Affairs* 28, no. 4 (2014): 409, https://doi.org/10.1017/S0892679414000586.

7 D. C. Lau, *Mencius, Revised ed.* (Penguin Books, 2004): 52.

8 Johannes G. de Casparis et al., "Art and Architecture," *History of Humanity volume V: From the Sixteenth Century to the Eighteenth Century*, ed. Peter Burke and Halil Inalcik (Routledge, 1994): 99.

9 Inazo Nitobe, *Bushido: The Soul of Japan* 12th ed. (Teibi Publishing Company, 1907): 42. Nitobe noted that "tenderness, pity and love, were traits which adorned the most sanguinary exploits of the samurai" quoting "It becometh not the fowler to slay the bird which takes refuge in his bosom".

a 'tragedy of goodwill', where well-intentioned data use inadvertently causes harm.

Natural Disaster Response and Data Protection

Humanitarian Need due to Natural Disasters in Asia-Pacific

According to the 2023 Global Natural Disaster Assessment Report, Asia had the largest number of disaster events in 2023, accounting for approximately 42 per cent of the natural disasters in the world.[10] In terms of the number of deaths attributed to disasters, Asia had the highest with 63,445 deaths, accounting for 73 per cent of the global total.[11] Countries across the Asia-Pacific frequently experience earthquakes, typhoons, and floods: earthquakes in Sichuan in 2008, Christchurch in 2011, East Japan in 2011, Nepal in 2015, and Myanmar in 2025; typhoon Haiyan in the Philippines in 2013; and the tsunami and flooding in the Indian Ocean in 2004, and in India–Bangladesh in 2022. All of these disasters required effective humanitarian responses to protect and assist vulnerable people in crisis and disaster. Thus, the response to natural disasters is an essential part of humanitarian activities in the Asia-Pacific.

Given the transborder nature of disasters, robust cross-border cooperation is indispensable to enabling effective international humanitarian activities. Following the Great East Japan Earthquake, the UN adopted the 'Sendai Framework for Disaster Risk Reduction 2015–2030' (the Framework), which set four priorities: understanding disaster risk, strengthening disaster risk governance to manage disaster risk, investing in disaster risk reduction for resilience, and enhancing disaster preparedness for effective response and to 'Build Back Better' in recovery, rehabilitation and reconstruction.[12] It is noteworthy that the Framework advances its objectives by promoting international cooperation, including 'access to and the sharing and use of non-sensitive data and information'.

The ASEAN Agreement on Disaster Management and Emergency Response (AADMER), which came into force in 2009, provides a comprehensive legal and institutional framework for regional cooperation, facilitating coordination, technical assistance, and the mobilisation of resources across all dimensions of disaster risk management and emergency response. Its Work

10 Academy of Disaster Reduction and Emergency Management et.al., *2023 Global Natural Disaster Assessment Report* (Beijing, 2024): 15, https://irdrinternational.org/upload/20241230/2023-global-natural-disaster-assessment-report.pdf.

11 Academy of Disaster Reduction and Emergency Management et.al., *2023 Global Natural Disaster Assessment Report.*

12 UN, *Sendai Framework for Disaster Risk Reduction 2015–2030* (2015), https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.

Programme 2021–2025 noted 'assisting humanitarian organizations' priority access to bandwidth, frequencies and satellite use for telecommunications and data transfer associated with disaster relief operations'.[13] While affirming the primary responsibility of domestic actors, these frameworks also facilitate the sharing of non-sensitive data and the creation of a common information system with international humanitarian organisations and affected stakeholders as a critical component of disaster response.[14] Given the 'state-centric method'[15] arising from State sovereignty and cultural, religious, and ethnic diversity within ASEAN, frameworks for the sharing of sensitive data have yet to be formalised. Nevertheless, establishing such mechanisms represents vital progress toward enhancing greater interoperability and effectiveness in humanitarian assistance across the region. Throughout these natural disasters across the Asia-Pacific region, mutual aid has been provided. For instance, common assistance was provided by community healthcare, through which nurses could strengthen mutual assistance and empower capacity-building of people in communities in Japan, Indonesia, and Nepal.[16]

The Pacific, consisting of numerous small island states, has cultivated a 'Pacific Way' – a mode of informal cooperation and relational governance in the aftermath of disasters – despite the region's complex post-colonial political and legal legacies.[17] Mutual assistance in these regions has ranged from everyday activities such as communications, cooking food, and cleaning debris away, to professional services of medical or nursing care, infectious disease assessment, and environmental hygiene.

Humanitarian assistance in disasters serves as a crucial source of support for those in need, leaving a lasting impression and memory for vulnerable and distressed people. Finding missing persons is a vital activity in disaster response. For instance, after the Great East Japan Earthquake, the Red Cross

13 ASEAN, *Agreement on Disaster Management and Emergency Response (AADMER) Work Programme 2021–2025* (2020), https://asean.org/wp-content/uploads/2021/08/AADMER-Work-Programme-2021-2025.pdf.

14 ASEAN, *Socio-Cultural Community Blueprint* (2025), https://www.asean.org/wp-content/uploads/2012/05/8.-March-2016-ASCC-Blueprint-2025.pdf.

15 Krishnakali Ghosh, Ranit Chatterjee, and Rajib Shaw, "Disaster Management Law and Agreement in ASEAN" *Disaster Law: Implications to Governance and Implementation* (Springer 2025): 52.

16 Yudi Ariesta Chandra et al., "Value of mutual assistance for disaster risk reduction in Japan, Indonesia, and Nepal: A preliminary study," *Health Emergency and Disaster Nursing* 7, no. 1 (2019), https://doi.org/10.24298/hedn.2018-0010.

17 W John Hopkins, "Indigenising international disaster law: a Pacific Way?" *Research Handbook on Disasters and International Law 2nd ed.*, ed. Marie Aronsson-Storrier and Susan C. Breau (Edward Elgar, 2024): 343, https://doi.org/10.4337/9781803924212.00027.

provided a 'Restoring Family Links' (RFL) website[18] to find and connect missing persons and family members or to inform that the affected people were safe in multiple languages (Japanese, English, Korean, Chinese, Portuguese, and Spanish). This platform serves to re-establish communication and maintain contact with family members or loved ones, free of charge. An RFL website was also used during the Nepal earthquake in 2015, the tsunamis in Indonesia in 2018 and 2021,[19] and the Noto Peninsula earthquake in 2024.[20] Together with the telephone-based disaster emergency message dial, digital platforms such as Google's Person Finder also served to connect persons after the 2011 Japanese earthquake. Statistics show that more people used social media (67.1 per cent) in the 2024 Noto Peninsula earthquake compared with the 2018 Kumamoto earthquake (37.9 per cent) when direct calling on mobile phones was the main tool (67.7 per cent).[21] Thus, restoring the infrastructure for social media and the online environment is essential in order to obtain information and reconnect people in a disaster.

International humanitarian law traditionally operates in the context of armed conflict. However, humanitarian responses are not limited to armed conflict but are naturally applied to situations of humanitarian emergencies, both in natural and man-made disasters. Thus, the pressing need for effective responses to natural disasters in the Asia-Pacific region has led to the application of humanitarian norms and operational expertise towards disaster response in non-conflict settings. It may be observed that a spirit of Asian solidarity or Pacific regional cooperation, grounded on its original communitarian principles, tends to emerge during times of disaster.

Public Interest and Vital Interest under Data Protection Laws

From a data protection point of view, the processing of the personal data of missing persons can be justified on the grounds of public interest as well as the vital interests of the data subject. Such processing is particularly essential for humanitarian purposes (EU GDPR Recital 46). No data protection law in the

18 International Committee of the Red Cross, *Reconnecting families: Preventing Separation, Searching for the Missing, Reuniting Loved Ones.* accessed 1 May 2025, https://www.icrc.org/en/what-we-do/reconnecting-families.

19 The RFL website was deployed three times in Indonesia: following the earthquake, tsunami, and liquefaction in Central Sulawesi (activated 2 October 2018), the tsunami in Banten (activated 23 December 2018), and the tsunami in West Sulawesi (activated 22 January 2021).

20 International Committee of the Red Cross, *ICRC and Japanese Red Cross helping to restore family links in Japan*. Accessed 1 May 2025, https://www.icrcnewsroom.org/story/en/31/icrc-and-japanese-red-cross-helping-restore-family-links-in-japan.

21 Ministry of Internal Affairs and Communications in Japan, *2024 White Paper on Information and Communications in Japan* (2024): 20. Accessed 1 May 2025. https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2024/pdf/00_fullversion.pdf.

Asia-Pacific region seems to explicitly include humanitarian purposes, except for the Philippine legislature's proposal in 2022 to add "humanitarian emergencies" as a lawful basis for processing sensitive data.[22] A few jurisdictions have delegated acts or administrative guidance on humanitarian provisions in a narrow scope. For instance, New Zealand has the Civil Defence National Emergencies (Information Sharing) Code 2013, which includes 'humanitarian assistance services' (6(1)(c)(iii)), the Australian Privacy (Australian Bushfires Disaster) Emergency Declaration (No. 1) 2020 temporarily (until 20 January 2021) authorised the use of personal data for humanitarian relief during a national crisis, and the Japanese Guidelines on the Handling of Personal Information in the Field of Disaster Risk Reduction allow for the sharing of data on vulnerable evacuees.[23]

Firstly, regarding general public interest, it can be exemplified, among others, as the state's 'important economic or financial interest, including monetary, budgetary and taxation matters, public health and social security'.[24] However, it should be noted that excessive reliance on public interest may lead to the erosion of private life and the misuse of personal data if the public interest and the interest of the individual whose data is processed are not fully aligned. In considering the balance between privacy and public interest, Covid-19 tracing applications were a controversial privacy topic in Asian jurisdictions.[25] The most famous Singaporean tracing app 'TraceTogether' could potentially infer geolocation data based on proximity to other users' devices, known as 'a hybrid decentralized-centralized, proximity-based approach'.[26] However, the TraceTogether app did not use GPS or internet connectivity, instead it provided sufficient privacy safeguards with a maximum 25-day data

22 House of Representatives of the Republic of the Philippines, *House Bill No. 898* (Pending with the Committee on Information and Communications Technology since 27 July 2022) (in English) Accessed 1 May 2025. https://docs.congress.hrep.online/legisdocs/basic_19/HB00898.pdf .

23 Cabinet Office, *Guidelines on the Handling of Personal Information in the Field of Disaster Risk Reduction* (2023). Accessed 1 May 2025, https://www.bousai.go.jp/taisaku/kojinjyouho/pdf/shishin.pdf

24 European Data Protection Board (EDPB), *Guidelines 10/2020 on restrictions under Article 23 GDPR Version 2.1* (2021): para 27.

25 For an example of privacy-preserving digital contact tracing using the DP3T protocol, which enforces purpose limitation through decentralised design and local processing of sensitive data, see Carmela Troncoso and Wouter Lueks, in Massimo Marelli, ed., *Handbook on Data Protection in Humanitarian Action*, 3rd ed. (Cambridge University Press, 2025): 80–82, Section 6.2.

26 Katie Hogan et al., "Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation," JMIR Medical Informatics 9, no. 7 (2021), https://doi.org/10.2196/27449.

retention period and strict prohibition on third-party sharing.[27] In contrast, the Malaysian MySejahtera app collected relatively more personal information, such as contact number, email address, full name, identity card, age, gender, ethnicity, and home address. It raised serious privacy concerns about digital surveillance for the purpose of public health. The lessons of the Covid-19 contact apps in Asia show that there are increasing public concerns about privacy protection even in the name of public interest or public health.[28] This is why, in addition to the selection of a suitable legal basis like public interest, it is crucial to ensure the application of all other data protection requirements and principles such as purpose limitation, data minimisation, and retention, and both transparent and proportionate digital utilisation of data with clear privacy rules must be particularly considered in balancing individual rights with public interest.

Second, as to the vital interest of an individual or other people, this means interest in saving, among others, a person's life, health, security, and dignity, such as urgent medical care for an unconscious individual. The vital interest may be an exception in ordinary life, but is not so unusual in humanitarian activities. In particular, during situations such as epidemics, natural disasters, or man-made crises, where rapid action is required to safeguard public health or individual safety, the protection of vital interests often justifies the processing of personal data without the individual's consent (for instance, GDPR Recital 46). Vital interest or protection of life is a commonly recognised legal basis across the Asia-Pacific region, including in countries such as Japan,[29] the

27 Jason Bay et al., BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders (Singapore: Government Technology Agency, 2020), https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf: Melyssa Eigen and Urs Gasser, Country Spotlight: Singapore's TraceTogether Program, July 20, 2020, https://cyber.harvard.edu/story/2020-07/country-spotlight-singapores-tracetogether-program?utm_source=chatgpt.com.

28 Melinda Martinus, "Smart City and Privacy Concerns During COVID-19: Lessons from Singapore, Malaysia, and Indonesia," *Smart Cities in Asia: Regulations, Problems, and Development*, ed. Thanh Phan and Daniela Damian (Springer, 2022): 45, https://doi.org/10.1007/978-981-19-1701-1_4.

29 Act on the Protection of Personal Information, No. 37 of 2021, Art. 18(3)(ii). (The provisions of the preceding two paragraphs do not apply in (ii) cases in which there is a need to protect the life, wellbeing, or property of an individual, and it is difficult to obtain the consent of the identifiable person).

Philippines,[30] Singapore,[31] South Korea,[32] and Thailand.[33] A series of natural disasters improved the practices of the sharing of personal data on the grounds of vital interests, overcoming the misconception that consent is the sole legal basis. Stakeholders became aware that personal data can be shared without consent when it is necessary to inform a private hospital physician of an individual's blood type when requiring an emergency transfusion or to notify family members if the individual becomes involved in a disaster or accident. This provision authorises flexibility in data protection laws to address urgent circumstances where the protection of a vital interest and safety must take precedence. As demonstrated by the disasters in the Asia-Pacific region, the processing of personal data for search-and-rescue operations, identification of survivors, or to provide medical treatment often relies on vital interests.

Information Sharing and Data Protection Principles

As mentioned above, in addition to the two legal grounds, it is imperative that data protection principles are upheld in the context of natural disasters. Such circumstances give rise to a number of concerns regarding the application of key data protection principles. First, data retention for emergency responses should be narrowly tailored within the emergency purpose. A resolution by the International Conference of Data Protection and Privacy Commissioners, now the Global Privacy Assembly (GPA), called for 'a proportionate approach' for emergency responses.[34] For instance, public bodies engaged in disaster response should have a disposal plan for personal information they have

30 Republic Act 10173, Data Privacy Act of 2012, Section 12(d). (The processing of personal information shall be permitted only if not otherwise prohibited by law, and when: (d) The processing is necessary to protect vitally important interests of the data subject, including life and health).

31 Personal Data Protection Act 2012, Art 21(3)(a). (Subject to subsection (3A), an organisation must not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information (as the case may be) could reasonably be expected to (a) threaten the safety or physical or mental health of an individual other than the individual who made the request).

32 Personal Information Protection Act, Act No. 19234, Art. 15(1)(5). (A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection: 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily, and property interests of a data subject or a third party). See also Art. 15(7).

33 Personal Data Protection Act, B.E. 2562 (2019) Sec. 24(2). (The Data Controller shall not collect Personal Data without the consent of the data subject, unless: (2) it is for preventing or suppressing a danger to a person's life, body or health). See also Section 4 of the same Act.

34 33rd International Conference of Data Protection and Privacy Commissioners, *Resolution on Data Protection and Major Natural Disasters* (2011), https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf.

obtained when it is no longer needed for the response. These balancing clarifications and compliance issues should be set out before emergencies and disasters by data protection authorities. The regional cooperation framework on data protection shared best practices through the Asia-Pacific Privacy Authorities (APPA), which was formed in 1992 and consists of privacy regulators from 21 jurisdictions or territories.[35]

Secondly, the risks associated with information sharing and the protection of individual privacy must be carefully considered or assessed in advance. A regional example can be found in the Japanese National Governors Association's 'Guidelines for the Publication of the Names of the Dead and Missing during Disasters'. These Guidelines authorise local governments to disclose the names of deceased and missing persons without obtaining prior consent from their families in the context of disaster response.[36] However, the Guidelines also explicitly warn of the risks that such disclosure may pose to individuals in vulnerable situations, such as victims of domestic violence or stalking. Although the Guidelines apply specifically to disaster response, the broader principle of balancing humanitarian needs with privacy and safety gained national attention following a tragic incident in which a domestic violence survivor was murdered shortly after a local government released her personal data. This disclosure occurred despite her request for confidentiality and outside the immediate scope of a disaster, yet the case underscored the very concerns highlighted in the Guidelines. The district court ultimately held the local government liable and awarded compensation for the breach.[37] This traumatic experience created hesitation among local governments to release personal data even for humanitarian activities in Japan. Victims in natural disasters are in a different situation; thus, a situational approach must be taken for humanitarian aid.

Thirdly, the cross-border sharing of information in disaster contexts presents intricate legal challenges, particularly within the constraints of urgent, time-sensitive operations. Disaster-related activities and the data flows that result cross many jurisdictional borders with different laws, ranging from no

35 Asia Pacific Privacy Authorities, 36th APPA Forum Communiqué, 1–2 December 2011. (The Conference endorsed a practical approach to information sharing in natural disasters and promoted ethical frameworks that enable data sharing). Accessed 1 May 2025, https://www.appaforum.org/forums/communiques/36th-appa-forum-communique/.

36 National Governors Association of Japan, *Guidelines for the Publication of the Names of the Dead and Missing during Disasters* (2021). Accessed 1 May 2025, https://www.nga.gr.jp/item/material/files/group/2/202106_4-3.pdf (in Japanese). 44 out of 47 prefectures had enacted guidelines or policies on sharing and protection of personal data in disasters as of January 2024.

37 *Judgement of Yokohama District Court Yokosuka Branch*, 15 January 2018, LEX-DB25549223. This case was not directly related to a disaster, yet served as a lesson of the worst-case scenario of sharing personal data by local governments.

comprehensive privacy protection laws to mandatory data localisation laws, often in unanticipated ways.[38] Research on disaster apps has revealed a significant gap between users' privacy expectations and the actual data practices of major apps, particularly the sharing of location data without user consent and without identifying the third-party recipients.[39] Furthermore, a security breach would undermine trust in cross-border data flow. For instance, the Singapore Red Cross data breach case illustrates the critical importance of adhering to both security and data retention obligations, with broader implications for fostering cross-border cooperation and maintaining trust in humanitarian data governance.[40] Based on the experience that sharing personal data can save or kill lives, it is vital for public-private stakeholders to develop 'a dynamic and situation-oriented understanding of vulnerability'[41] and to prepare and consult in advance on the sharing and protection of personal data in the event of a disaster.

Emerging Technologies and Humanitarian Action

Biometric Data as 'Asiatic despotism'

Biometric use in Asia originated in Bengal, India in 1897 when the Calcutta Police employed fingerprinting for criminal identification. This practice was later expanded across Asia, a region sometimes associated with the concept of 'Asiatic despotism'.[42] The use of biometric data, including facial recognition systems, in locating missing persons as part of disaster response efforts raises significant and often controversial concerns from a data protection perspective. Biometric identification was employed by the Thai Victim Identification Information Management Centre after a tsunami in 2004 with support from Interpol. The report indicated that dental identification was useful, followed

38 Joel R. Reidenberg et al., *Privacy and Missing Persons after Natural Disasters*, Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars (2013): 11, https://www.wilsoncenter.org/publication/privacy-and-missing-persons-after-natural-disasters.

39 Madelyn R. Sanfilippo, et. al., "Disaster Privacy/Privacy Disaster," *Journal of the Association for Information Science and Technology* 71, no. 9 (2020): 1002, https://doi.org/10.1002/asi.24353.

40 Singapore Data Protection Commission, Singapore Red Cross Society [2020] SGPDPC 16. Accessed 1 May 2025, https://www.singaporelawwatch.sg/Portals/0/Docs/Judgments/2020/[2020]%20SGPDPC%2016.pdf.

41 Christian Henrik Alexander Kuran et al., "Vulnerability and Vulnerable Groups from an Intersectionality Perspective," *International Journal of Disaster Risk Reduction* 50 (2020), https://doi.org/10.1016/j.ijdrr.2020.101826.

42 Keith Breckenridge, *The Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present* (Cambridge University Press, 2014): 63.

by fingerprints, DNA, and physical characteristics.[43] In India, it is reported that in 2018, the Delhi Police used a facial recognition system to identify and rescue approximately 3,000 missing children in just four days.[44] However, the 'function creep' shows that the Indian law enforcement agency began deploying the software to investigate other cases such as the 2022 Delhi riots and the 2021 Red Fort violence.[45] Similar stories are found in China: a two-year-old boy abducted in 1988 was located 32 years later through the use of facial recognition technology together with DNA testing, which simulated age-related changes in his appearance over time.[46] At the same time, facial recognition software was used for a different purpose to stop toilet paper thieves at the Temple of Heaven Park in Beijing.[47]

Function creep is defined as a phenomenon of the expansion of a system or technology beyond its original purposes in a way that was apparently unforeseen by its developers, users, or the public.[48] A single piece of personal data can serve multiple functions beyond the gaze of the data subject. Biometric data may technically be capable of serving multiple functions, ranging from authentication to biometric surveillance, often without the data subject's awareness or consent, which may be termed as 'overpurposed by design'.[49] 'Behaviometrics',[50] such as signature verification, typing rhythm, keystroke

43 Kirsty Wright et al., "An Evaluation of the Thai Tsunami Victim Identification DNA Operation," *Forensic Science Policy & Management* 6, no. 3/4 (2015): 69, https://doi.org/10.1080/19409044.2015.1068887.

44 PTI "Facial Recognition Systems Helps Trace 3,000 Missing Children in 4 Days," *The Times of India*, 22 April 2018. Accessed 1 May 2025, https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms.

45 Intifada P. Basheer, "Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India" *Journal of Development Policy and Practice* 10, no. 1 (2024): 61, 70, https://doi.org/10.1177/24551333241283992.

46 Suyin Haynes, "After 32 Years, a Missing Son Is Reunited With His Parents in China," *TIME*, 19 May 2020. Accessed 26 May 2025, https://time.com/5838768/missing-man-reunites-parents-china/. It did not give details about the database or the process of how the photos were compared. CNN, "Facial Recognition Helps Reunite Kidnapped Toddler with Family After 32 Years," 19 May 2020. Accessed 1 May 2025, https://edition.cnn.com/2020/05/19/asia/china-kidnapped-son-reunited-intl-hnk#:~:text=A%20man%20who%20was%20abducted,'an%2C%20in%20Shaanxi%20province.

47 AJ Willingham and Nanlin Fang, "Chinese park installs facial recognition software to stop toilet paper thieves," *CNN*, 21 March 2017. Accessed 1 May 2025, https://edition.cnn.com/2017/03/20/world/china-toilet-paper-thieves-face-recognition-trnd/index.html.

48 Bert-Jaap Koops, "The Concept of Function Creep," *Law, Innovation and Technology* 13 no. 1 (2021): 29, https://doi.org/10.1080/17579961.2021.1898299.

49 International Committee of the Red Cross, "Digital Dilemmas Debate #7: Biometrics – 'Overpurposed' by design?" 30 September 2021. Accessed 1 May 2025, https://www.icrc.org/en/digitharium/digital-dilemmas-debate-7.

50 Omer Tene, "Privacy: The New Generations," *International Data Privacy Law* 1 (2011): 15, 21, https://doi.org/10.1093/idpl/ipq003.

analysis, and gait recognition, are increasingly employed in authentication or potentially locating missing persons,[51] yet they are also vulnerable to misuse for law enforcement and commercial or marketing purposes.[52] Data protection wisdom has established a principle of purpose limitation that 'personal data [be] collected for one specific purpose and in order to fulfil one function'.[53] Data recontextualisation through a new smart device or system is prohibited unless the new purpose is compatible with the original purpose(s) in a predictable manner,[54] thereby reinforcing the rule of law.

Biometric authentication for humanitarian aid is not inherently a threat to individual privacy and integrity.[55] However, humanitarian organisations increasingly recognise that when the purposes of data use or the partners involved change significantly, it may be necessary to inform beneficiaries and, depending on applicable consent protocols, obtain renewed or additional consent from data subjects.[56] As highlighted in the concept of 'surveillance humanitarianism',[57] the use of biometric data for secondary purposes, such as surveillance or biometric categorisation for evaluative or decision-making processes, risks undermining individual dignity and autonomy, extending beyond the data subject's control and reasonable expectations. Therefore, the use of biometric data must be strictly limited to what is necessary for the intended humanitarian purpose and safeguarded by robust security measures. The privacy formula in the Puttaswamy case issued by the Supreme Court of

51 See e.g. Alireza Sepas-Moghaddam and Ali Etemad, "Deep Gait Recognition: A Survey," *arXiv* (2022), https://doi.org/10.48550/arXiv.2102.09546; Pawel Kasprowski, Zaneta Borowska, and Katarzyna Harezlak, "Biometric Identification Based on Keystroke Dynamics," *Sensors* 22, no. 9 (2022), https://doi.org/10.3390/s22093158.

52 In the investigation of the Gauri Lankesh assassination in India, forensic gait analysis of an individual's walking pattern as a biometric identifier was employed as an innovative technique to identify a suspect whose facial features were obscured. See Kamakshi Tiwari, "Digital Revolution in Criminal Procedure of India: An in-Depth Examination of the Impact of Emerging Technologies," *International Journal of Law Management & Humanities* 6 (2023): 3573, 3578, https://doij.org/10.10000/IJLMH.116540.

53 Maria Tzanou, "The EU as an Emerging 'Surveillance Society': The Function Creep Case Study and Challenges to Privacy and Data Protection," *Vienna Journal on International Constitutional Law* 4 (2010): 407, 421, https://research.edgehill.ac.uk/en/publications/the-eu-as-an-emerging-surveillance-society-the-function-creep-cas-2.

54 Article 29 Data Protection Working Party, "Opinion 03/2013 on Purpose Limitation," 2 April 2013, 11.

55 Keren Weitzberg et al., "Between Surveillance and Recognition: Rethinking Digital Identity in Aid," *Big Data & Society* 8, no. 1 (2021), https://doi.org/10.1177/20539517211006744.

56 Ben Hayes, "Migration and Data Protection: Doing No Harm in an Age of Mass Displacement, Mass Surveillance and 'Big Data'," *International Review of the Red Cross* 99 (2017): 179, 198, https://doi.org/10.1017/S1816383117000637.

57 Mark Latonero, "Stop Surveillance Humanitarianism," *The New York Times*, 11 July 2019. Accessed 1 May 2025, https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

India reviewed the constitutional validity and upheld a partial uncostitutionality by limiting private use of the biometric-based identity system in India known as Aadhaar, representing "foundation" or "base" in Hindi. The judgement seems to have created a slim overlapping consensus, while still diverging, to some degree, among Asian law communities where it is frequently referred to. In short, any restriction of the fundamental right to privacy must meet the following requirements; 1) the existence of law, 2) the necessity of a legitimate State aim, and 3) proportionality.[58] Facial identification technologies often lack a clear legal basis and proportionality, while only the necessity condition, such as finding missing persons, is satisfied. In cases involving biometric identification tools, it is the secondary purpose that should be rigorously scrutinised by data protection authorities and courts to prevent function creep.

In relation to prohibited artificial intelligence (AI) practices under the EU AI Act (Regulation (EU) 2024/1689), the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement is listed as a prohibited category. However, the use of such AI systems may be allowed under the strict necessity test for the targeted search for specific victims of abduction, trafficking in human beings, or sexual exploitation of human beings, as well as the search for missing persons (EU AI Act Art. 5(1)(h)(i)). The provision generally applies to law enforcement authorities as they search for victims of serious crimes and try to locate missing persons. While this provision does not directly apply to humanitarian organisations, they may be able to use facial recognition systems to search for missing persons at least in a strictly necessary situation (EU AI Act Recital 24). In the Asia-Pacific region, while several AI-related laws and numerous guidelines and soft-law instruments have established frameworks for the use of facial recognition systems, none appears to explicitly prohibit their deployment.[59]

Biometric Data as "Asiatic despotism"

Satellite Images and Privacy Protection

Technologies such as those for satellite imagery can generate high-resolution maps and detailed visuals of disaster-affected areas. Satellite images enable search and rescue teams to pinpoint zones requiring urgent assistance even

58 *Judgement of the Supreme Court of India*, *Justice K.S. Puttaswamy (Retd) vs Union of India* [2017] 10 SCC 1. The judgement, relying on life and personal libery under Article 21 of the Indian Constituion, categorised the right to privacy as right to physical body, right to informational self-determination, and right to decisional autonomy. See Sara M. Smyth, *Biometrics, Surveillance and the Law* (Routledge, 2019) 106-137.

59 China introduced "Security Management Measures for the Application of Facial Recognition Technology," entering into force on 1 June 2025. Accessed 1 May 2025, https://www.chinalawtranslate.com/en/facial-rec-2025/.

in situations where terrestrial infrastructure, such as electricity, is disrupted or entirely unavailable. Remote sensing technologies are also used as a means of proof in environmental monitoring, which is particularly useful on remote islands.[60] In addition to its application in situational assessments related to armed conflict and environmental monitoring, satellite imagery can significantly enhance disaster response operations and humanitarian activities, including the prevention or mitigation of risks to vulnerable populations in Sudan.[61]

The UN's Principles Relating to Remote Sensing of the Earth from Outer Space note that '[r]emote sensing shall promote the protection of mankind from natural disasters'.[62] In the earthquakes in Turkey and Syria, the United Nations Satellite Centre (UNOSAT) reported that the space community worked together to provide critical information and support to the affected countries.[63] These capabilities support search and rescue operations by facilitating the identification of areas in critical need and providing essential information on the damage to inform the prioritisation and coordination of the humanitarian response.

However, the advent of high-resolution satellite imagery obtained from outer space introduces emerging privacy challenges as a disaster response measure, particularly with respect to the adequacy of existing legal frameworks to regulate the incidental or intentional capture of personal data from orbital vantage points. It was noted that only certain types of sensors, such as optical sensors, which produce images instantly, or Synthetic Aperture Radar (SAR) sensors, the data from which can be processed to generate images, are currently capable of visualising data that may be used immediately and which may constitute directly or indirectly identifiable personal data.[64] Nevertheless, continued advancements in sensor technologies will clear the fog at some point. Even if a satellite image does not directly identify a specific individual, it may still enable indirect identification when combined with other data sources, such as residential registry information linked to a building's location

60 Maria Maniadaki et al., "Reconciling Remote Sensing Technologies with Personal Data and Privacy Protection in the European Union: Recent Developments in Greek Legislation and Application Perspectives in Environmental Law," *Laws 2021* 10 (2021), https://doi.org/10.3390/laws10020033.

61 Nathaniel A. Raymond et al., "While We Watched: Assessing the Impact of the Satellite Sentinel Project," *The Georgetown Journal of International Affairs* 185 (2013), http://www.jstor.org/stable/43134425.

62 United Nations, *Resolution 41/65: Principles Relating to Remote Sensing of the Earth from Outer Space* (1986), https://www.unoosa.org/pdf/gares/ARES_41_65E.pdf.

63 United Nations Satellite Centre (UNOSAT), "Marash/Antep earthquake (6 February 2023, M 7.8)". Accessed 1 May 2025, https://unosat.org/products/3480.

64 Luigi Izzo, "EO Satellite Data Management and Privacy Law" *European Journal of Privacy Law & Technologies* 2024 (2024): 219, 227, https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1970/1514.

or the consumption data of electricity collected through a home sensor.[65] This technological development calls for the re-examination of existing privacy laws and regulatory gaps in light of the expanding capabilities of remote sensing systems.[66]

Within the intersection of space law and data protection law, Article VI of the Outer Space Treaty, which requires 'authorization and continuing supervision by the appropriate State Party' including for those activities conducted by non-governmental entities, can be interpreted in a manner that complements existing data protection regimes. Data protection authorities can play a critical role in ensuring compliance with domestic and international data protection frameworks where satellite technologies involve the collection of personally identifiable information. Their oversight is essential to establishing accountability, enforcing legal safeguards against unintended consequences of advanced remote sensing capabilities on data protection and privacy, and placing privacy by design in high-resolution remote sensing from space-based platforms, such as requirements for blurring personal identifying information in satellite images.[67] Cyber-attacks on satellites and collisions between satellites and other objects should also be considered within the existing Sendai Framework.[68]

Internet Governance and Human Control in the Asia-Pacific Regions

Online Harm and Internet Governance

Social media has played a pivotal role in enhancing humanitarian operations, including the dissemination of critical information, needs mapping, real-time situation reporting, volunteer mobilisation, family reunification, and fundraising efforts. Nonetheless, it has also facilitated the rapid spread

65 Souichirou Kozuka and Mayu Terada, "Data Law Aspects of Commercial Satellite Remote Sensing: New Challenges for the New Opportunities," *Proceedings of the International Institute of Space Law 2020* (2020): 243, 246, https://doi.org/10.5553/IISL/2020063003002.

66 Megan M. Coffer, "Balancing Privacy Rights and the Production of High-Quality Satellite Imagery," *Environmental Science & Technology* 54 (2020), https://pubs.acs.org/doi/10.1021/acs.est.0c02365.

67 Temitope Lawal, Melanie Jackson, and Eugenia Georgiades, "Privacy in the Age of Remote Sensing During Natural Disasters in Australia and Indonesia," *Digital Law Journal* 4, no. 2 (2023): 15, 35, https://doi.org/10.38044/2686-9136-2023-4-2-15-39; Rachel McAmis et al., "Over Fences and Into Yards: Privacy Threats and Concerns of Commercial Satellites," *Proceedings on Privacy Enhancing Technologies* (2024), https://doi.org/10.56553/popets-2024-0022.

68 Jessie Hamill-Stewart, "The Sendai Framework and Satellite Security," *International Journal of Disaster Risk Science* 16 (2025): 117, https://doi.org/10.1007/s13753-025-00614-9.

of misinformation and disinformation, which can undermine the credibility, coordination, and overall effectiveness of humanitarian responses.[69] Noteworthy regional approaches to social media regulation by imposing intermediary liability have emerged across the Asia-Pacific region, reflecting diverse legal traditions, governance models, and socio-political priorities. For instance, following the Christchurch mosque shootings in New Zealand, Australia introduced the Sharing of Abhorrent Violent Material Act of 2019 through the Criminal Code Amendment. On 20 March 2025, the Perth District Court sentenced a Western Australian man to three years' imprisonment for disseminating violent extremist material produced by the Islamic State via online platforms.[70] In Australia, the eSafety Commissioner holds broad authority to issue removal notices for online content, including material that constitutes hate speech. Australia has taken a pioneering role in implementing age-based restrictions on social media use, introducing measures to create an account for individuals under the age of 16 as part of its broader efforts to enhance online protection for minors under the Online Safety Amendment Act 2024. This approach to internet governance reflects key norms and characteristics of Australia's legal and political culture, particularly its emphasis on pragmatic harm reduction, principles of fairness, and the pursuit of democratic security.[71]

However, generative AI has been used to create fabricated images, such as imaginary floods or lions escaping from zoos during disasters, which have rapidly spread misinformation and can have harmful effects, particularly on minors.[72] Japan's pragmatic approach appears more moderate than Australia's, aiming to strike a careful balance between the protection of free speech and the regulation of online harms, particularly those affecting individuals.

China, as the most developed regulatory model, implements social media surveillance through a structured framework grounded in multiple national

69 Aleksandrina V. Mavrodieva and Rajib Shaw, "Social Media in Disaster Management," *Media and Disaster Risk Reduction*, ed. Rajib Shaw, Suvendrini Kakuchi, Miki Yamaji (Springer, 2021): 55, https://doi.org/10.1007/978-981-16-0285-6_4.

70 The Australian Federal Police, "WA man First Person Convicted for Transmitting Violent Extremist Material Online," 20 March 2025. Accessed 1 May 2025, https://www.afp.gov.au/news-centre/media-release/wa-man-first-person-convicted-transmitting-violent-extremist-material.

71 It is beyond the scope of this chapter, but the Australian internet governance laws are regarded as experiments in digital constitutionalism. See Monique Mann and Angus Murray, "Digital Constitutionalism in Australia," ed. Giovanni De Gregorio, Oreste Pollicino, and Peggy Valcke, *The Oxford Handbook of Digital Constitutionalism* (Oxford University Press, forthcoming). Accessed 1 May 2025, https://doi.org/10.1093/oxfordhb/9780198877820.013.42.

72 Kentaro Takeda, "An Outlier in Asia? Why Japanese People Don't See Fake News as a Serious Threat," *Fake News Across Asian Countries*, ed. by Edson C. Tandoc Jr. (Routledge, 2025): 161.

laws.[73] Politically sensitive or harmful content is subject to extensive censorship, enforced both by government authorities and internal moderators employed by internet service providers.[74] The internet, like AI-generated content, is strategically used, sometimes misused, as a tool for 'geopolitical ends'[75] and political stability in China, which may potentially conflict with humanitarian activities, particularly where critical voices risk suppression for political reasons.[76] Furthermore, China has data localisation rules that oblige critical information infrastructure operators to retain personal data within Chinese territory.[77]

Humanitarian organisations often engage in negotiations with State authorities to coordinate their operations with national regulations. In contrast, social media platforms operate under distinct regulatory frameworks governed by various jurisdictions, leading to complexities in compliance against not just '5.24 billion'[78] human users, but also 'an army of bots'.[79] With attention to such regulatory inconsistencies, humanitarian organisations are being pressed to respond in ways that align with the characteristics of social media. In short, the fragmented internet governance frameworks and digital divide across Asia-Pacific regions require international humanitarian organisations to coordinate their operations, challenging Euro-centric narratives of the humanitarian system in the name of 'humanitarian diplomacy in the Asia-Pacific'.[80]

73 Chengxin Peng and Guosong Shao, *Privacy and Data Protection Law in China* (Wolters Kluwer 2024).

74 Yuner Zhu, "Social Media and State Surveillance in China: The Interplay between Authorities, Businesses and Citizens," *Constitutionalising Social Media*, ed. by Edoardo Celeste and Clara Iglesias Keller (Hart Publishing, 2022): 199, https://doi.org/10.5040/9781509953738.ch-012.

75 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023): 295.

76 Angela Huyue Zhang, "Agility Over Stability: China's Great Reversal in Regulating the "Platform Economy," *Harvard International Law Journal* 63, no. 2 (Spring 2022): 457, https://dx.doi.org/10.2139/ssrn.3892642.

77 Personal Information Protection Law Art. 40 (Critical information infrastructure operators and the personal information processors that process personal information up to the amount prescribed by the national cyberspace department shall store domestically the personal information collected and generated within the territory of the People's Republic of China).

78 Simon Kemp, *Digital 2025: Global Overview Report*, 5 February 2025, https://datareportal.com/reports/digital-2025-global-overview-report.

79 Jack M. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation," *UC Davis Law Review* 51 no. 3 (2018): 1149, 1175, https://dx.doi.org/10.2139/ssrn.3038939.

80 Alistair DB Cook and Lina Gong, "Humanitarian Diplomacy in the Asia-Pacific: Part I," *Asian Journal of Comparative Politics* 6, no. 3 (2021): 183, https://doi.org/10.1177/20578911211045668.

Online Harm and Internet Governance

Algorithmic Regulations by Human Oversight

Algorithm-curated content streams in social media are not politically neutral.[81] They are sometimes shaped, in the worst cases distorted or polluted, by harmful or extremist communities or automated bots. The echo chamber of radical discourse poses difficult legal issues regarding free speech and personalisation in relation to data protection law. In Myanmar, which lacks a data law to protect users' privacy, it was reported that Facebook posts were used to amplify the hatred and violence in communal conflicts and for surveillance of users to control communications.[82] This surveillance is part of a broader system in which the military Government exercised the 'power to conduct searches, seizures, and arrests and to extend detention without judicial oversight'.[83] In addition, as the UN noted, 'in Myanmar, State inaction against incitement to genocide may contribute to very serious consequences for vulnerable communities'.[84] The UN human rights Special Rapporteurs emphasised that under a 'digital dictatorship', '[o]nline access to information is a matter of life and death for many people in Myanmar, including … the millions trying to navigate a devastating economic and humanitarian crisis'.[85] While the whitelist scheme of partial restoration of internet services contributes to economic transactions, the blocking of major social media services hinders humanitarian activities. The legal status of social media platforms under international human rights law is opaque, often not being accountable due to potential tension with State sovereignty.[86]

81 Ferenc Huszár et al., "Algorithmic Amplification of Politics on Twitter," *Proceedings of the National Academy of Sciences* 119, no. 1 (2021), https://doi.org/10.1073/pnas.2025334119.

82 Business for Social Responsibility (BSR), "Human Rights Impact Assessment: Facebook in Myanmar," (2018). Accessed on 1 May 2025,https://about.fb.com/wp-content/uploads/2018/11/bsr-facebook-myanmar-hria_final.pdf.

83 Ei Thandar Bo and Khin Thitsar Aung, "Myanmar," *Privacy and Personal Data Protection Law in Asia*, ed. Adrian Mak et al. (Hart, 2025): 250.

84 UN, Note by the Secretary-General, *Promotion and Protection of the Right to Freedom of Opinion and Expression (A/74/486)*, 9 October 2019, para. 25, https://digitallibrary.un.org/record/3833657?v=pdf.

85 UN, Myanmar: UN experts condemn military's "digital dictatorship", 7 June 2022, https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship. Myanmar's Cybersecurity Law, entering into force in 2025, grants sweeping powers to military authorities to surveil digital communications, including a penalty of one to three years' imprisonment for the use of Virtual Private Networks (VPNs). See Nicholas Coppel and Lennon Y. C. Chang, *Myanmar's Digital Coup* (Springer, 2024): 42.

86 Thanapat Chatinakrob, "Rethinking the Scope of International Law Regulating Information Operations: Lessons Learned from a Crime of Online Genocide in Myanmar," *Cambridge International Law Journal* 11, no. 2 (2022): 243, https://doi.org/10.4337/cilj.2022.02.05.

The Myanmar case starkly illustrates the consequences of such regulatory deficiencies in protecting personal data, requiring the urgent need for comprehensive human rights due diligence by global technology companies, particularly in jurisdictions not aligned with international human rights norms. While liability models may differ, the primary responsibility for conducting human rights impact assessments lies with social media platforms.[87] However, the task becomes particularly challenging and difficult in contexts under military rule or within ethnically, even linguistically,[88] divided jurisdictions, where political instability or social conflicts hinder the evaluation process. Social media companies failed to take into account the country's complex sociopolitical and ethnic landscape due to reliance on majority-language standards.[89] In situations of deeply divided conflict, maintaining the impartiality and independence of content moderation is often challenging. In these instances, humanitarian organisations can offer valuable support by sharing contextual experience and operational insights that help platforms better understand the specificities of armed conflict, humanitarian action, the needs and vulnerabilities of affected populations, and the impact of harmful information in those settings.[90] If necessary, they can also provide critical

87 Eve Gaumond and Catherine Régis, "Assessing Impacts of AI on Human Rights: It's Not Solely About Privacy and Nondiscrimination," LAWFARE, 27 January 2023, https://www.lawfaremedia.org/article/assessing-impacts-of-ai-on-human-rights-it-s-not-solely-about-privacy-and-nondiscrimination. For different intermediary liability models, see Caio C. V. Machado and Thaís Helena Aguiar, "Emerging Regulations on Content Moderation and Misinformation Policies of Online Media Platforms: Accommodating the Duty of Care into Intermediary Liability Models," *Business & Human Rights Journal* 8 no. 2 (2023): 244, https://doi.org/10.1017/bhj.2023.25.

88 Content moderation requires different languages and dialects within Myanmar. See Rebecca J. Hamilton, "Platform-Enabled Crimes: Pluralizing Accountability When Social Media Companies Enable Perpetrators to Commit Atrocities," *Boston College Law Review* 63, no. 4 (2022): 1349, 1364, https://digitalcommons.wcl.american.edu/facsch_lawrev/2220.

89 Jenifer Whitten-Woodring et al., "Poison If You Don't Know How to Use It: Facebook, Democracy, and Human Rights in Myanmar," *The International Journal of Press/Politics* 25 no. 3 (2020): 407, http://dx.doi.org/10.1177/1940161220919666; Aim Sinpeng et al., *Facebook: Regulating Hate Speech in the Asia Pacific* (2021): 27, https://r2pasiapacific.org/files/7099/2021_Facebook_hate_speech_Asia_report.pdf; Hesam Nourooz Pour, "Transitional Justice and Online Social Platforms: Facebook and the Rohingya Genocide" *International Journal of Law and Information Technology* 31 issue 2 (2023): 95, 105, https://dx.doi.org/10.2139/ssrn.5256580; Rajika L. Shah, "The Consequences of Inaction: An Inquiry into International Criminal Liability of Social Media Comapnies for Artsakh 2020," Journal of International Media & Entertainment Law 10 no.2 (2024) 20: amp; https://www.swlaw.edu/sites/default/files/2024-12/Shah%20Article-%20JIMEL%2010.2%20-%20Final%2012.19%20%281%29.pdf.

90 However, the responsibility for content moderation should remain with the platforms themselves; humanitarian organisations have neither the mandate nor the operational means to undertake such tasks. See for instance, International Committee of the Red Cross, *Addressing Harmful Information in Conflict Settings: A Response Framework for*

data with the aim of bringing more humanity to social media platforms, such as warning indicators of conflicts and information on populations in need of humanitarian assistance, and risk analyses that social media companies may be unable to gather themselves due to political or logistical constraints. Human rights impact assessment extends beyond a mere technical tool for algorithmic oversight; it must also account for social, cultural, and ethical contexts. This is especially crucial in cases like Myanmar, where the chronic plight of the Rohingya required a nuanced approach to mitigate or prevent human rights harms.[91] Social media regulation has increasingly shifted toward a polycentric framework of networked governance, distinct from direct censorship. This evolution reflects a shift from a first-generation framework premised on the traditional relationship between government and the individual, to a second-generation trilateral structure encompassing the government, digital platforms, and the individual user.[92] Within this evolving regulatory landscape, humanitarian organisations can play a crucial role in a culturally sensitive approach in bridging the gap between social media companies, government, and local people, minorities, and those who are vulnerable.

The European notion of human dignity may require normative adaptation to resonate with the culturally embedded values of Asian societies.[93] Human oversight as a 'socio-technical'[94] tool should incorporate the assessment of social, cultural, and ethical contexts apart from the negotiation with local government. This approach is also evident in the Asia-Pacific where 'a harmony-based approach de-emphasises individuals'[95] in assessing civic and societal impacts on communities or ethnic groups, such as the Myanmar case

Humanitarian Organizations (Geneva: ICRC, 2024), https://www.icrc.org/en/publication/addressing-harmful-information-conflict-settings-response-framework-humanitarian.

91 Mark Latonero and Aaina Agarwal, "Human Rights Impact Assessments for AI," *Carr Center Discussion Paper* (2021): 7. Accessed 1 May 2025, https://www.hks.harvard.edu/sites/default/files/2023-11/2021_13_facebook-failure-in-myanmar_0.pdf.

92 Jack M. Balkin, "Old-School /New School Speech Regulation," *Harvard Law Review* 127 no. 8 (2014): 2296, https://harvardlawreview.org/wp-content/uploads/2014/06/vol127_balkin.pdf.

93 Hiroshi Miyashita, "Human-centric Data Protection Laws and Policies: A Lesson from Japan," *Computer Law and Security Review* 40 (2021), https://doi.org/10.1016/j.clsr.2020.105487 (noting that "if human centrism is a part of European human dignity, then a similar concept known as 'respect' has already been introduced in constitutional theory as well as in the Japanese policy papers").

94 Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Springer, 2022): 79, https://iasalut.cat/wp-content/uploads/2023/02/Beyond-Data-Human-Rights-Ethical-and-Social-Impact-Assessment-in-AI.pdf.

95 Andrew McStay, "Emotional AI, Ethics, and Japanese Spice: Contributing Community, Wholeness, Sincerity, and Heart," *Philosophy & Technology* 34 (2021): 1781, 1799, https://doi.org/10.1007/s13347-021-00487-y.

where divisiveness on social media may be reproduced and amplified with 'no consideration of local context, country- or region-specific meanings'.[96] While concepts such as human oversight and control may align with European frameworks, they must also integrate 'historic Indigenous ethical thought'[97] within the process of impact assessment. For instance, the Indigenous AI Initiative in the name of Māori data sovereignty is actively engaged in developing culturally attuned AI technologies that serve the needs and values of Indigenous communities, with a particular focus on applications such as language revitalisation and environmental stewardship.[98] The recognition and implementation of Indigenous peoples' rights in Southeast Asia remain uneven, particularly concerning critical areas such as employment, livelihood, healthcare, and food security.[99] In the absence of inclusive policy frameworks, these disparities risk being further entrenched by algorithmic systems that reflect existing structural inequalities. Diversity and inclusiveness must be central to algorithmic regulatory regimes.[100] These approaches reflect a regional convergence toward embedding human oversight and inclusive values as fundamental safeguards in algorithmic governance.

Conclusion

A sufficient knowledge of data protection laws and preparation in data protection governance will avoid the 'tragedy of good will',[101] which causes harm through the use of personal data. The lessons of the Asia-Pacific region reflect that data protection and humanitarian action can be seen as 'compatible, complementary to, and supporting each other'.[102]

Two key considerations emerge. First, in responding to natural disasters, assistance must be tailored to the situational vulnerabilities of affected individuals, though recognising that traditional categories such as location,

96 Richard Ashby Wilson and Molly K. Land, "Hate Speech on Social Media: Content Moderation in Context," *Connecticut Law Review* 52, no. 3 (2021): 1029, 1060, https://ssrn.com/abstract=3690616.

97 McStay, "Emotional AI," 1782.

98 Spencer Lilley et al., "Māori Data Sovereignty: Contributions to Data Cultures in the Government Sector in New Zealand," *Information, Communication & Society* 27, no. 16 (2024): 2801, https://doi.org/10.1080/1369118X.2024.2302987.

99 Isabel Inguanzo, "The Rights of Indigenous Peoples in Southeast Asia," *The Palgrave Handbook of Political Norms in Southeast Asia*, ed. Gabriel Facal, Elsa Lafaye de Micheaux, Astrid Norén-Nilsson (Palgrave Macmillan, 2024): 357.

100 UNESCO, *Missing Links in AI Governance* (2023): 136, https://www.unesco.org/en/articles/missing-links-ai-governance.

101 Luciano Floridi, "Information Technologies and the Tragedy of the Good Will," *Ethics and Information Technologies* 8 (2006): 253, 254, https://doi.org/10.1007/s10676-006-9110-6.

102 Marelli, ed., *Handbook on Data Protection*, 66.

age, or gender may be insufficient. Factors such as experiences of domestic violence, child abuse, or membership in politically persecuted or ethnically divided communities demand heightened sensitivity and protections. Upholding professional confidentiality fosters trust in the ethical handling of personal data during humanitarian operations. Second, the increasing reliance on algorithmic or automated data processing and surveillance technologies presents new challenges, particularly in regions with limited oversight. To mitigate risks and harms, human rights/data protection impact assessments should be mandated for high-risk AI systems, with human oversight playing a central role in ensuring transparency and accountability. Ultimately, the protection of human rights must remain the foundation upon which humanitarian actions are built.[103]

103 Inter-Agency Standing Committee (IASC), *Operational Guidelines on the Protection of Persons in Situations of Natural Disasters* (2011): 13, https://www.refworld.org/policy/legalguidance/brookings/2011/en/83748.

PART 5

Building Capacity and Addressing Challenges Ahead

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

19

TEACHING DATA PROTECTION AS TRUST-BUILDING

Cosimo Monda and Cristina Teleki

Introduction

Data-driven technology is transforming most existing structures into polycentric systems of governance, whereby "a pull on one strand will distribute tensions after a complicated pattern throughout the web as a whole".[1] Trust plays a crucial role in these novel polycentric structures because data may act either as a bottleneck or as a pipeline. Trust is the only differentiator between the two. In data-driven polycentric structures of governance based on trust, data flows amongst the various centres based on preordained rules and principles. On the contrary, in polycentric structures of governance that lack trust concerning the collection and sharing of data, the lack of trust becomes a bottleneck that can lead to the breakdown of the whole structure.

The importance of trust has been recognised by a number of regulators. The European Union (EU) recognised early on that data protection rules were an enabler of trust-building in the EU and beyond.[2] Moreover, the EU recognises that the General Data Protection Regulation (GDPR)[3] has

1 Lon Fuller, "The Forms and Limits of Adjudication," *Harvard Law Review* 92 (1978): 353–409, https://classactionsargentina.com/wp-content/uploads/2020/07/fuller_the-forms-and-limits...-policc3a9ntricos.pdf.

2 European Commission. "Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock," Communication from the Commission to the European Parliament and the Council, COM (2019) 374 final, 24 July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0374.

3 European Parliament and Council of the European Union. "General Data Protection Regulation," Regulation (EU) 2016/679, 27 April 2016, Official Journal of the European Union, L 119, 4 May 2016, 1–88, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

DOI: 10.4324/9781003650164-27

created "a solid framework for digital trust".[4] In addition, in January 2019, then Japanese Prime Minister Abe Shinzo spoke about Data Free Flow with Trust (DFFT) at the World Economic Forum as a new model for global data governance. The DFFT concept, simply put, is to promote the free flow of data across borders while ensuring trust in privacy, security, and intellectual property.[5] These policy documents recognise learning and awareness-raising as an important aspect of trust-building.[6]

The humanitarian sector has not been sheltered from this development. Not only has the nature of war changed,[7] the actors operating within the humanitarian space have changed as well.[8] In current military conflicts, businesses and private individuals[9] have come to play roles unimaginable earlier.[10] These actors challenge existing notions of power and bring along operational principles, cultures, and strategies that may be incompatible with the principles enclosing the humanitarian space. In addition, data permeates and informs responses across the humanitarian sector.[11] Indeed, the delivery of humanitarian assistance necessitates the collection and processing of significant amounts of personal data. This data, encompassing sensitive information such as medical records, biometric data, and location details, is crucial for needs assessments, aid distribution, and protection activities. Scholars writing on humanitarian extractivism have critiqued this phenomenon for diminishing trust in humanitarian action, arguing that humanitarians are moving

4 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data* (COM(2020) 66 final). EUR-Lex, 19 February 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066.

5 Ministry of Foreign Affairs of Japan, *Data Free Flow with Trust*, 28 June 2019, https://www.mofa.go.jp/ecm/ec/page4e_000973.html

6 European Commission. "Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock," Communication from the Commission to the European Parliament and the Council, COM (2019) 374 final, 7, 24 July 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0374

7 Herfried Münkler, *The New Wars* (Patrick Camiller trans., Polity 2005).

8 Daniel Thürer, "Dunant's Pyramid: Thoughts on the "Humanitarian Space"," *International Review of the Red Cross* 89, no. 47 (2007), https://international-review.icrc.org/sites/default/files/irrc-865-3.pdf.

9 The Economist, "How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare," 5 January 2023, https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

10 Aaron Martin and Quito Tsui, "Humanitarian Connectivity in Crisis," *Global Policy Journal*, 2 June 2025, www.globalpolicyjournal.com/blog/02/06/2025/humanitarian-connectivity-crisis.

11 Larissa Fast, "Governing Data: Relationships, Trust & Ethics in Leveraging Data & Technology in Service of Humanitarian Health Delivery," *Daedalus* 152, no. 125 (2023), https://doi.org/10.1162/daed_a_01996.

away from directly providing material aid to facilitating emerging markets through their use of emerging technologies and partnerships with business.[12]

The importance of trust has been acknowledged in the humanitarian sector for a while. 'Trust in humanitarian action' was the top item on the agenda of the 33rd International Conference of the Red Cross, which took place in 2019. The Conference acknowledged that trust – of the people and communities it serves, of the authorities it works with, and of the general public – was the foundation of humanitarian action, ensuring access to people in need, support, and respect for the humanitarian mission. The reason for such a thematic choice was the widespread perception of a "declining trust in institutions and governments, an increase in public scrutiny, and calls for stronger integrity and accountability".[13] The Conference emphasised the fact that access to populations affected by armed conflict, disasters, or crises requires significant trust in impartial humanitarian action by all parties. It concluded that "trust is both a fragile and a two-way process, which means that understanding and being close to communities is essential".[14] Despite the focus on trust, the 33rd International Conference of the Red Cross failed to take into account the importance of data practices in relation to the issue of trust in humanitarian action. This was remedied a year later, when the Group of Friends of the Protection of Civilians in Armed Conflict argued for a link between trust and a safe information structure to conduct humanitarian action. In particular, they declared that:

> The trust of the people they [humanitarian organizations] serve is the currency of humanitarian organizations. This trust is a precondition for humanitarian action. Therefore, we, as Members States, must create an environment, including a safe information infrastructure that allows humanitarian organizations to successfully carry out their mandate. The Resolution on Restoring Family Links adopted at the 33rd International Conference of the Red Cross and Red Crescent in 2019 constitutes an important step in this direction.[15]

12 Kristin Bergtora Sandvik, *Humanitarian Extractivism: The Digital Transformation of Aid* (1st ed., Manchester University Press 2023); Elisa Pascucci, "More Logistics, Less Aid: Humanitarian-Business Partnerships and Sustainability in the Refugee Camp," *World Development* 142 (2021): 105424, https://doi.org/10.1016/j.worlddev.2021.105424.

13 ICRC. 2019a. "Trust in Humanitarian Action—Statutory Meetings," 33rd International Conference, https://rcrcconference.org/about/33rd-international-conference/trust-in-humanitarian-action/.

14 33rd International Conference of the Red Cross and Red Crescent. "Summary Report from Commission III: Trust in Humanitarian Action," 9–12 December 2019, Geneva, Switzerland.

15 Switzerland, Mission to the United Nations, "Joint Statement by the Group of Friends of the Protection of Civilians on Cyber-Attacks Against Critical Infrastructure," United

This call to action followed longstanding scholarship highlighting the uneasy relationship between trust and digital technology.[16]

A few humanitarian organisations have been at the forefront of addressing these challenges by adapting their rules and *modus operandi*. In terms of rules, the International Committee of the Red Cross (ICRC) has already pioneered the ICRC Rules on Data Protection in 2015. In terms of *modus operandi*, in 2020 the ICRC established a partnership with the European Centre on Privacy and Cybersecurity (ECPC) based at the Faculty of Law of Maastricht University. The partnership was signed to provide privacy and data protection training to staff of the ICRC, the Red Cross/Red Crescent national societies, and other humanitarian agencies. Scholars have recently highlighted that the ICRC has encouraged university collaboration with legal experts, both for research into the question of rules and how to communicate them.[17] The ICRC-ECPC partnership has thus been the result of efforts to both professionalise the humanitarian employees working with data and to fill a gap in the market for providers of training services, which, until the partnership, had not tailored curricula to the sector's needs.[18]

This chapter sets out to argue that teaching data protection increases trust in humanitarian action. To support this argument, it first outlines the pedagogical approach employed in ICRC–ECPC training programmes, particularly the Data Protection Officer in Humanitarian Action (DPOHA) initiative. It then develops a normative argument that data protection education can act as a form of institutional trust-building, reinforcing accountability to affected populations and aligning humanitarian operations with core values of dignity and human rights.

Teaching data protection in humanitarian contexts, however, presents distinct challenges and requirements. Unlike professionals in regulatory, academic, or corporate sectors, humanitarian staff often engage with personal data as part of direct service delivery in complex, high-risk environments. For

Nations Security Council Arria Formula, 26 August 2020, https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-organizations/un/swiss-speeches-statements.html/content/missions/mission-new-york/en/meta/speeches/2020/august/26/joint-statement-by-the-group-of-friends-of-the-protection-of-civ.

16 Mariarosaria Taddeo, "Trust in Technology: A Distinctive and a Problematic Relation," *Knowledge, Technology & Policy* 23 (2010): 283, https://doi.org/10.1007/s12130-010-9113-9.

17 Julian Antouly et al., "The challenges of research in the humanitarian sector: An evolving relationship," *International Review of the Red Cross* 106 no. 926 (2024): 525–541, https://international-review.icrc.org/sites/default/files/reviews-pdf/2024-12/the-challenges-of-research-in-the-humanitarian-sector-926.pdf.

18 Valérie Gorin, "Humanitarian Studies: A Field Still in the Making," *Humanitarian Alternatives*, no. 25 (2024), https://www.alternatives-humanitaires.org/en/2024/03/20/humanitarian-studies-a-field-still-in-the-making/.

them, data is not merely a legal object or compliance matter, but an element of human relationships, protection, and vulnerability. Accordingly, effective training in these contexts must go beyond legal doctrine. It must highlight the human consequences of data practices, using scenarios and examples that make the ethical stakes of data protection tangible. Over time, the DPOHA method has evolved to reflect this reality, emphasising experiential learning, narrative framing, and real-world dilemmas. This enables participants to internalise data protection not simply as a legal requirement, but as a form of principled humanitarian practice.

Teaching Data Protection to Humanitarian Workers

The ICRC-ECPC partnership acknowledges that trust is the natural outcome of knowledge, proximity, and community. These have thus become the core deliverables of the partnership that has materialised as an in-person training programme and a community of practice.

The DPOHA was developed in response to the growing need for specialised data protection expertise in the humanitarian sector. It builds directly on the foundation laid by the ICRC Rules on Personal Data Protection and the Handbook on Data Protection in Humanitarian Action, which has been developed as part of a cross-sector initiative bringing together all major humanitarian organisations, academia, regulators, tech sector companies, and civil society.[19] The purpose of this certification is to train and certify data protection officers specifically for work in humanitarian contexts, addressing the unique challenges that arise when collecting and processing personal data during humanitarian operations.

The DPOHA employs Maastricht University's well-known Problem-Based Learning (PBL) pedagogy.[20] The key aspects of the PBL approach in this certification include active learning through real-world scenarios, hands-on application, and case studies. In this sense, participants in the DPOHA are actively engaged with real-life issues and scenarios specific to humanitarian contexts. Rather than passively receiving information, they work through practical problems that data protection officers would face in humanitarian operations. Second, the programme emphasises practical application with a focus on "do's and don'ts" rather than just theoretical knowledge. Participants learn by doing and applying their knowledge to concrete situations. Third, participants work in groups on case studies under the supervision of tutors

19 Massimo Marelli ed., ICRC, *Handbook on Data Protection in Humanitarian Action*, 3rd edition (Cambridge, Cambridge University Press, 2024), https://doi.org/10.1017/9781009414630.

20 More information can be found here: https://www.maastrichtuniversity.nl/over-de-um/onderwijs-aan-de-um/problem-based-learning.

who evaluate both group outcomes and individual performance. The case studies address unique and recent situations and challenges found in humanitarian contexts, such as the use of biometric data.[21]

The DPOHA is offered in a blended learning format. Before the in-person component, participants complete preparatory work covering foundational topics such as the origins of data protection principles, the right to privacy, and the relevance of data protection in humanitarian action. Second, the main component of the DPOHA is a one-week in-person training course that provides detailed instruction and hands-on practice.

Rather than narrowly focusing on one legal framework in particular, the ECPC has adopted a methodological approach that enables comprehensive privacy analysis across diverse contexts. Through structured analysis rather than rigid rule-following, this teaching method centres on empowering humanitarian practitioners to properly understand and mitigate privacy risks to beneficiaries and institutions and to embrace compliance at all operational stages through analytical thinking. This method places data as the central point of consideration, ensuring that privacy analysis becomes an integral part of humanitarian decision-making regardless of the specific legal context.

It is worth highlighting that this pedagogical approach has the advantage of preventing groupthink. If all humanitarian professionals were trained in the same data protection framework, alternative perspectives on data management, ethical considerations, or innovative solutions may be overlooked. This in turn may lead to two sets of negative consequences. On the one hand, groupthink can lead to overconfidence in shared assumptions, underestimation of risks, or ignoring novel data protection challenges. On the other hand, groupthink can replace the continuous improvement of data protection practices – which is required by the dynamic nature of this field – with complacency.

In order to deliver on the PBL method and to prevent groupthink, the DPOHA has engaged a diverse teaching team. Scholars and practitioners from the ECPC have been joined by professionals and practitioners from the ICRC, the World Food Program (WFP), United Nations High Commissioner for Refugees (UNHCR), and United Nations Office for Coordination of Humanitarian Affairs (OCHA), the International Federation of Red Cross and Red Crescent Societies (IFRC), the Luxembourg Red Cross, and the *Ecole Polytechnique fédérale de Lausanne* (EPFL). These experts have created and adapted the DPOHA curriculum over the years. This has resulted in the creation of a course that remains unique in the industry.

More than 600 people have attended the DPOHA since 2021. DPOHA participants are often employed in middle and high management positions.

21 Chapter 4, "The Logic of Biometrics and Organisational Accountability".

The geographic representation is impressive, unique, and impossible to replicate, with participants coming from all corners of the world, including Afghanistan, Mali, and Iraq. DPOHA course participants primarily come from the National Red Cross and Red Crescent Societies, the ICRC, IFRC, WFP, UNHCR, OCHA, and the International Organization for Migration (IOM). Participants typically hold positions such as data protection officers or those designated to take on this role, information management specialists, programme managers dealing with sensitive data, IT and digital security professionals working in humanitarian contexts, and legal and compliance personnel. In addition, numerous experts in Restoring Family Links (RFL) have attended the course.[22] This became particularly important in light of the fact that the 33rd International Conference adopted the Resolution "Restoring Family Links while respecting privacy, including as it relates to personal data protection".[23] This Resolution reaffirmed the specific role of the International Red Cross and Red Crescent Movement in RFL and in cooperation with States in this field, including recognition of the Movement's need to process and transfer personal data for exclusively humanitarian purposes.[24] These efforts have been supported by the Government of Luxembourg that highlighted the need to protect people's digital dignity and to respect the principle of do no harm at all times.[25]

The DPOHA has been conducted with the support of the Directorate for Development Cooperation and Humanitarian Affairs of the Luxembourg Ministry of Foreign and European Affairs across four continents, with participants representing a wide range of countries and regions. In order to ensure a balanced geographical presence, to date the DPOHA has been delivered in Italy, Switzerland, Jordan, Turkey, Thailand, Kenya, Senegal, Mexico, Costa Rica, and Argentina. Although the course is taught in English, the DPOHA has also been offered in French, Arabic, and Spanish.

22 RFL is the term given by the International Red Cross and Red Crescent Movement to the range of activities that aim to prevent separation and disappearance, clarify the fate and whereabouts of missing persons, restore and maintain contact between family members, and facilitate family reunification whenever possible.

23 33rd International Conference of the Red Cross and Red Crescent. "Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection." Resolution 33IC/19/R4, 9–12 December 2019, Geneva, Switzerland, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

24 33rd International Conference of the Red Cross and Red Crescent. "Restoring Family Links while Respecting Privacy".

25 Government of Luxembourg. *Engagement sur le renforcement de la protection des données dans l'action humanitaire*, International Conference of the Red Cross and Red Crescent (2020), https://rcrcconference.org/pledge/engagement-sur-le-renforcement-de-la-protection-des-donnees-dans-laction-humanitaire/

DPOHA participants have the possibility to join an online community of practice (CoP). The CoP was designed to answer requests from the alumni of the DPOHA certification course who expressed the need to continuously enhance their knowledge and be part of a network of humanitarian professionals working in the field of privacy and cybersecurity. The CoP provides a shared space for humanitarian professionals to communicate and share information, stories, and personal experiences related to the implementation of a privacy and cybersecurity compliance programme or actions in their organisations in a way that builds trust.

The DPOHA has posed two main challenges over the years. The first concerns the need to tailor it to a diverse global workforce. According to the Active Learning Network for Accountability and Performance (ALNAP), there were an estimated 5,000 organisations in the humanitarian system in 2021, roughly 10% higher than estimated a decade ago. While the largest humanitarian agencies are a well-established part of the international system, many smaller ones come and go as crisis situations escalate and subside, along with the funding and international partnerships that they bring.[26] In addition, more than 630,000 humanitarian staff were estimated to be working in countries with humanitarian crises in 2020. Over 90% of these staff were nationals of the countries in which they were working in.[27] This workforce is composed of a variety of professions ranging from security personnel to drivers. The level of professionalisation of the various roles composing the humanitarian workforce remains a challenge. In addition, due to the ongoing digitalisation process in the world, most of these professionals will face data protection issues in their work. To meet these challenges, the DPOHA has evolved from an advanced course in data protection that was offered during its first iterations to a course that provides foundational knowledge in data protection, including the main actors, data transfers, and the sound management of a data breach. In addition, the DPOHA has been built around practical case studies that all humanitarians encounter during their careers, such as cash programmes or RFL programs that involve the collection and management of large amounts of personal data.

The second and related challenge concerns the scaling up of the CoP. The CoP achieved at least three of its initial goals: connecting people, providing a shared context, and enabling dialogue amongst its members. A number of follow-up workshops about data protection in the humanitarian context have been organised for CoP members. However, while the CoP shows promise, scaling efforts have been tempered by resource considerations. As with any

26 ALNAP (2022) *The State of the Humanitarian System*. ALNAP Study. London: ALNAP/ODI, 55, https://alnap.org/help-library/sohs-2022/.

27 ALNAP, *The State of the Humanitarian System*, 63.

platform, the CoP requires regular updates and engagement to make it a viable resource. In addition, scaling efforts have been influenced by linguistic diversity considerations and the need for culturally appropriate communication. The CoP has the potential to become a high-trust network of humanitarian professionals where learning and exchange take place regularly. This would, however, require an investment of resources that for the time being could not be prioritised.

Evidence-based conclusions about the impact of the DPOHA would be premature and are in any case beyond the scope of this chapter. Nevertheless, one can make a few inferences based on existing scholarship and feedback from participants. The DPOHA blends formal and personal knowledge and has evolved into a collaborative space for knowledge transfer.[28] First, there is the knowledge shared between the trainers and the participants. This transfer ensures that policy instruments in the participating institutions are known, understood, and mainstreamed. Second, there is a knowledge transfer that takes place amongst the trainers themselves. This ensures the emergence of best practices and the establishment of coordination channels amongst the participating humanitarian agencies. Third, there is a knowledge transfer from the participants in the DPOHA to the trainers and among the participants themselves. Privacy and data protection considerations vary across cultures and communities. What one society considers acceptable data sharing might be viewed as invasive surveillance in another. Local customs, religious considerations, and historical experiences with government surveillance all influence appropriate privacy practices. The DPOHA training encourages participants to share examples from their local cultures and to build bridges between different cultures. Lastly, the DPOHA enables a transfer of knowledge from the participants towards their local communities. In this way, the participants in the DPOHA courses act as knowledge multipliers in their local contexts, becoming privacy and data protection pioneers or leaders.

Teaching Data Protection as Trust-Building

This chapter started by arguing that trust plays a crucial role in data-driven polycentric structures of governance. Interestingly, trust has been a subject of study for a number of disciplines. The origins of trust in economics and philosophy focused on how people develop trust in each other. Trust was seen as an interpersonal relationship based upon experiences such as lending

28 Étienne Wenger-Trayner, *Communities of Practice: Learning, Meaning, and Identity* (18th printing, Cambridge University Press, 2008). Michael Polanyi, *Personal Knowledge: Towards a Post-Critical Philosophy* (University of Chicago Press, 2009).

money or business ties.[29] The literature on trust expanded rapidly from the 1970s onwards. Putnam's discussion of social capital put trust at the centre of a collection of positive behaviours, such as participation in voluntary associations, civic participation (including voting), and participation in informal social networks.[30]

Trust has been a topic of increased interest to scholars of humanitarian affairs as well. Hugo Slim distinguishes between operational trust, which he describes as interpersonal and intimate, and accountability trust, which derives from internal control mechanisms meant to ensure financial transparency and sanction bad behaviour.[31] We posit that teaching data protection to humanitarian staff contributes both to operational trust and to accountability trust as understood by Slim. We suggest, however, that teaching data protection to humanitarian staff goes beyond the procedural view of accountability that Slim supports to cover substantive accountability as well. In particular, we suggest that teaching data protection to humanitarian workers increases the accountability to donors and accountability to affected people. We outline these differences in the following paragraphs.

First, teaching data protection contributes to the emergence and maintenance of operational trust in humanitarian action. It is well-accepted that successful digitalisation processes depend on employees accepting and trusting the new technology.[32] Teaching data protection early in the process of technology adoption demystifies data-driven technology and empowers humanitarian workers to understand its pertinence for humanitarian operations. This empowers humanitarian staff to answer the communities' questions about the fate of the data that they collect. The DPOHA training offers space to understand data-driven technology and to apply data protection principles in humanitarian contexts. For example, data is often collected by humanitarian workers during cash distribution operations. A number of departments with different mandates are involved in such operations: the data protection officer, protection, assistance, and cooperation. When humanitarian workers are trained in data protection principles, they can perform the task of data

29 Eric M Uslaner (ed.), *The Oxford Handbook of Social and Political Trust* (Oxford University Press 2018): 5.

30 Robert D. Putnam, Robert Leonardi, and Raffaella Nanetti, *Making Democracy Work: Civic Traditions in Modern Italy* (Princeton University Press, 1994). Robert D. Putnam, "Bowling Alone: The Collapse and Revival of American Community," *Proceedings of the 2000 ACM Conference on Computer Supported Cooperative Work*, accessed 1 March 2025 (ACM 2000), https://doi.org/10.1145/358916.361990.

31 ICRC. "Trust Me – I'm a Humanitarian," *Humanitarian Law & Policy Blog*, 24 October 2019, https://blogs.icrc.org/law-and-policy/2019/10/24/trust-humanitarian/.

32 Andrea Bencsik, Dávid Máté Hargitai, and Anastasia Kulachinskaya, "Trust in and Risk of Technology in Organizational Digitalization," *Risks* 10, no. 5 (2022): 90, https://www.mdpi.com/2227-9091/10/5/90.

collection efficiently, understanding the type of data they need to collect and relying on the principle of data minimisation at all times. In addition, data protection training can ensure swift coordination among the various departments involved in cash transfer operations on data protection matters.

In addition, teaching data protection contributes to operational trust in humanitarian action by increasing inter-agency trust. As the work of the OCHA shows, humanitarian crises involve a number of domestic and international actors that work hand in hand to provide assistance and protection to affected people. The coordination efforts will inevitably involve dialogue about the data collected by each humanitarian agency. Teaching data protection allows humanitarian professionals – who have diverse educational backgrounds – to have access to the same knowledge pool and to speak a common language when it comes to managing, sharing, and protecting personal data. This, in turn, can increase the inter-agency trust and cooperation on data-related matters.[33]

Second, in addition to the markers of accountability described by Slim, teaching data protection contributes to accountability trust in two ways – accountability to donors and accountability to affected people. Data protection has become an integral part of the constitutional orders of many countries that financially support humanitarian action and humanitarian actors.[34] The DPOHA training empowers humanitarian professionals to become accountable to their donors in relation to the data collected and processed during humanitarian operations.

Data protection training supports accountability to affected people in a number of ways. The DPOHA training method is human-centric and grounded in the principle that fundamental rights and human dignity must be respected at all times. Participants are not simply taught compliance frameworks, but are socialised into ways of collecting and processing personal data that reflect these normative values. Through structured reflection, case studies, and peer dialogue, they gain a rights-based sensitivity that is central to ethical data practice.

In addition, the DPOHA training approach raises awareness of the risks associated with mishandling personal data. As highlighted in other chapters of this collection,[35] data breaches are not merely technical failures – they rep-

33 An example of this can be found here: UNHCR, WFP, and UNICEF. "Trilateral Data Sharing Agreement for Cash Assistance," *UNHCR Media*, https://www.unhcr.org/media/trilateral-data-sharing-agreement-cash-assistance-unhcr-wfp-unicef.

34 European Data Protection Supervisor, *Two Decades of Personal Data Protection, What next?: EDPS 20th Anniversary*, accessed 22 May 2025 (Publications Office 2024), https://data.europa.eu/doi/10.2804/652641.

35 See Chapter 11, "Data protection in the framework of Restoring Family Links humanitarian activities: Code of conduct, resolutions, and data breaches" and Chapter 12, "By the

resent significant breaches of trust that carry reputational consequences and undermine the social legitimacy of humanitarian operations. These ruptures are well-studied in the literature, and underscore the need for robust preventative and responsive measures.

The training therefore goes beyond awareness-raising by providing practical content on how to mitigate such risks through the application of mature data protection principles. Participants are empowered to handle complex incidents, including the procedural and ethical dimensions of informing data subjects in the event of a breach. These measures – when internalised and implemented – strengthen the accountability of humanitarian organisations to affected populations and promote a culture of transparency and trustworthiness. More broadly, teaching data protection can be understood as a knowledge pipeline that contributes to the professionalisation of humanitarian data governance. The DPOHA training is delivered by seasoned practitioners – many of whom have backgrounds in access to information, cybersecurity, or humanitarian affairs – and this interdisciplinary expertise enables a pedagogical approach grounded in real-world problem-solving. Moreover, the field of data protection is rapidly evolving, moving from earlier narratives of data stewardship to contemporary understandings rooted in fiduciary duty and trust-based governance. The training environment offers a unique opportunity to capture, organise, and transmit these new regulatory, ethical, and operational paradigms into a coherent body of knowledge. In doing so, it reinforces the idea that trust is not a given, but a consequence of accountable and rights-respecting data practices – and that teaching data protection is central to achieving this outcome.

Conclusion

The humanitarian sector is not an island. On the contrary, it has become a part of domestic politics and policy-making in many countries. In addition, the humanitarian sector has become a data-driven polycentric governance structure where trust plays a crucial role. Trust in such structures is a tool that can prevent tensions from rippling into unpredictable and damaging waves. In addition, trust ensures the stability of the web of relations. Finally, when ripples occur – such as in a situation of a data breach – trust allows actors to identify counterparts and perform damage control. The questions about trust in data-related technology cannot be answered in a vacuum in the humanitarian sector. The DPOHA training and its ensuing community of practice are premised on the idea that teaching data protection will increase and secure trust

Book, Beyond and Backwards? Ethical considerations on the 2022 data breach affecting the Family Links Network of the Red Cross Red Crescent Movement".

in data-intensive operations, as some humanitarian operations have become. By building analytical competencies throughout organisations, the DPOHA training fosters a culture where privacy considerations become embedded in operational thinking rather than treated as mere compliance checkboxes. This contribution has suggested that this ultimately leads to more trust through the protection of beneficiary data across the humanitarian ecosystem.

The experience of delivering data protection training to humanitarian professionals reveals critical insights for future pedagogy. Most notably, it underscores that training content must be responsive to the operational realities and ethical sensitivities of the humanitarian sector. In environments where staff are navigating crises, working under pressure, and making rapid decisions, abstract legalism is often insufficient. What proves more effective are case-based discussions and concrete illustrations of harm and benefit – for instance, how inadequate data safeguards can lead to exclusion from aid, or how responsible data sharing can facilitate family reunification. Such pedagogical strategies support the internalisation of data protection as a core humanitarian value, closely linked to protection, dignity, and trust. The DPOHA programme exemplifies this shift, showing that teaching data protection in humanitarian settings is not merely about transmitting knowledge, but about transforming practice. It requires the integration of legal, ethical, and operational dimensions in a way that resonates with practitioners' lived experiences. In this sense, teaching data protection is more than a compliance exercise, it is a trust-building intervention that helps embed accountability in both institutional culture and individual decision-making.

20

DATA PROTECTION IN THE TIMES OF ARTIFICIAL INTELLIGENCE

Towards a Digital Humanism

Wojciech Wiewiórowski with the contributions from Olivier Matter and Michèle Dubrocard

Human dignity is fragile.[1] This perspective should be at the core of reflections on potentially harmful data processing practices, especially in the context of the development of artificial intelligence (AI).

Such fragility is exacerbated by crisis situations, when people need humanitarian assistance. Moreover, the multiplication of protracted crises around the world has aggravated the vulnerability of affected people, who are forced to flee their homes and become refugees, asylum seekers, or migrants.

The classic narrative about AI, combining real promise but also risks, is also relevant in the field of humanitarian action, but is precisely magnified by the sense of urgency and emergency. On the one hand, AI systems may help improve the efficiency of the assistance provided by humanitarian organisations. On the other, the use of such systems may have disastrous short- and long-term impacts on the lives of individuals who are already vulnerable and in a situation of increased dependence on those who help them.

In addition, the humanitarian space is not immune from the evolution of our digital world and increased interconnection among people. In this regard, affected communities can be privileged targets for misinformation and disinformation, notably through social media, among other data-driven harms.

In recent years, the European Union (EU) has adopted a number of new regulations in order to create a safer digital space and protect the fundamental

1 European Data Protection Supervisor (EDPS), keynote speech, Brussels Privacy Symposium, "Vulnerable People, Marginalization and Data Protection," 15 November 2022, https://www.edps.europa.eu/system/files/2022-11/22-11-15_brussels_privacy_symposium_en.pdf.

DOI: 10.4324/9781003650164-28

rights of users online. The Digital Services Act[2] and the Digital Markets Act[3] aim at addressing the challenges posed by digital platforms, including the need to fight hate speech and the spread of disinformation.

Even more recently, the new legal framework adopted on 13 June 2024 in the area of AI aims to promote "the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection".[4] However, the ambition displayed from the first recital of the AI Act is mitigated by the implicit recognition of possible conflict with other legislation: according to Recital 45 of the Regulation, "(p)ractices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation".

It is clear that data protection and AI are heavily interlinked. However, data protection and privacy do not merge, nor disperse into AI.

Data protection and privacy should be defended against the risk of confusing or muddling them amidst the AI hype, as this could mean dangerously weakening these fundamental rights. Of course, AI is fuelled by data, much of which some operators refuse to recognise as 'personal' because (they claim) this data has been aggregated or anonymised. But the aims of AI and data protection regulation are different.

The AI Act is conceived and framed as internal market legislation for commercialising AI systems, which is completely different from a regulation such as the General Data Protection Regulation (GDPR) designed to protect the fundamental rights and freedoms of individuals as regards the processing of their personal data.

It must also be kept in mind that the EU AI Act does not apply in a vacuum and is part of a broader legal framework that contains protection for individuals affected by AI systems. Notably, the qualification of an AI system as "high-risk" in the AI Act does not mean that its deployment is lawful, even if the specific safeguards imposed by the AI Act are implemented. Instead, such

2 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, 1–102.

3 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, 1–66.

4 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) 300/2008, (EU) 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024.

qualification indicates a need for greater scrutiny, including from the perspective of EU data protection law where personal data is being processed.

In addition, the enforcement of AI rules is not accompanied by the same safeguards that come with the enforcement of data protection rules. This is the case, for example, with the independence of a data protection authority, which is guaranteed by Article 8(3) of the Charter of Fundamental Rights of the European Union.

Respect for data protection and privacy is the essential prerequisite to put people at the centre and *ahead* of technology. We must defend the identity of data protection in order to protect humanity. Data protection is a compass for the development of a digital humanism, allowing for a smoother digital transformation that actually serves the interests of humankind. It should guide all of us in the digital age, or more precisely in the 'infosphere', described by Luciano Floridi as a space "that is seamlessly analogue and digital, offline and online".[5]

Against this background, the example – out of many possible examples – of the management of the EU's external borders and of the treatment of asylum seekers and migrants in the digital age is of particular relevance to examine the new challenges arising from the use of AI in the area of humanitarian action. As duly noted by Ana Beduschi,[6] "contemporary humanitarian crises tend to be increasingly complex and protracted, transcending the boundaries between humanitarian aid and development cooperation". The EU could thus be directly impacted by humanitarian crises that originate far from its borders.

In its Strategy 2020–2024, the European Data Protection Supervisor (EDPS) already stressed that "data protection is one of the last lines of defence for vulnerable individuals, such as migrants and asylum seekers approaching EU external borders".[7] The adoption, in May 2024, of the EU Pact on Asylum and Migration, which is grounded in the interoperability of the EU's large-scale IT systems as well as on AI tools, will profoundly change the way people in need of humanitarian aid can be identified.

5 Luciano Floridi, Soft Ethics and the Governance of the Digital, *Philos. Technol.* 31, no. 1–8 (2018), https://doi.org/10.1007/s13347-018-0303-9.

6 Ana Beduschi, *Harnessing the potential of artificial intelligence for humanitarian action: opportunities and risks*, 2022, published by Cambridge University Press on behalf of the ICRC.

7 EDPS Strategy 2020–2024, Shaping a Safer Digital Future, 19, https://www.edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf.

AI and Data Protection in the Context of Migration

The management of the EU's external borders and the way individuals' personal information related to migration and asylum matters is collected, used, and stored will be subject to the principle of interoperability among the EU's large-scale IT systems. But interoperability is about far more than just linking these systems. It is also essential for the deployment of AI technologies, notably the integration of automated decision-making, algorithmic profiling, and the processing of biometric data.

The processing of biometric data, because of its uniqueness and immutable nature, requires a higher level of protection in order to safeguard individuals against adverse effects of its use, especially when these individuals are among the most vulnerable. Both the EU's data protection legal framework and the Council of Europe's Modernised Convention 108, as well as many other data protection frameworks around the world, including those applicable to international organisations, have recognised the sensitive nature of biometric data,[8] which is subject to specific protection.

In the EU, the AI Act laid down prohibitions on certain uses of remote biometric identification and on emotion recognition systems. However, these bans do not seem sufficient,[9] especially if they are applied to individuals who are already vulnerable.

Remote Biometric Identification of Individuals in Publicly Accessible Spaces

The EDPS has repeatedly expressed concern as regards remote biometric identification of individuals in publicly accessible spaces, in light of a high risk of intrusion into individuals' private lives.[10] The EDPS has strong reservations about whether such large-scale systems meet the necessity and proportionality requirements and could therefore be considered acceptable interference with fundamental rights.[11]

Article 5(1)(h) of the AI Act prohibits the use of real-time biometric identification systems in 'publicly accessible spaces' for the purpose of law

8 See Chapter 4, "The logic of biometrics and organisational accountability".

9 EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office, 19 December 2025, https://www.edps.europa.eu/system/files/2025-01/2024-12-18_submission_ai_board_on_prohibitions_en.pdf.

10 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), issued on 18 June 2021, paras. 30–32, https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

11 EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices, page 10, https://www.edps.europa.eu/system/files/2025-01/2024-12-18_submission_ai_board_on_prohibitions_en.pdf.

enforcement. The EDPS notes, however, that Recital 19 of the AI Act specifies that 'publicly accessible spaces should not include prisons or border control'. The exclusion of crossing-points or areas dedicated to border control might be particularly detrimental to the rights of people on the move. Another issue not clarified by the AI Act is the status of refugee camps and it is still open to debate whether they should be considered publicly accessible spaces or not.

Such questions are not purely hypothetical, especially in light of the growing interest of EU Member States as well as Frontex in comprehensive border surveillance systems, in order to 'provide pre-frontier situational awareness beyond maritime and land borders'.[12] A few years ago, the EU funded the 'Roborder project',[13] aiming to develop and demonstrate a fully functional autonomous border surveillance system. The system was supposed to use unmanned mobile robots and ground vehicles operating both independently and in swarms, incorporating additional sensors as part of an interoperable network.

Emotion Recognition AI Systems

The EDPS has constantly warned against the use of emotion recognition AI systems,[14] and recommended their prohibition. Any technology that is used to infer human emotions raises serious issues of necessity and proportionality because of the sensitivity of human emotions and their effect on human dignity. Here again, we are not in a purely fictional scenario, in light of the former EU-funded iBorderCtrl research project,[15] which has since been abandoned.

Article 5(1)(f) of the AI Act expressly prohibits both the use and the placing on the market of AI systems that infer emotions of a natural person in the areas of workplace and education. However, the EDPS considers that the rationale for the prohibition of emotion recognition in workplaces and schools, namely the imbalance of power, is even more applicable and relevant to other contexts, among which the field of border control, migration, and asylum, closely connected to humanitarian action. Those who are forced to escape from conflicts, natural disasters, or climate change have no choice but to try and resettle in other places of the world, as refugees, asylum seekers, or migrants.

12 NESTOR: "Showcasing a new border surveillance system," https://www.frontex.europa.eu/innovation/eu-research/news-and-events/nestor-showcasing-a-new-border-surveillance-system-NIV4SC.

13 "Intelligent robots for border protection," https://cordis.europa.eu/project/id/740593.

14 EDPB-EDPS Joint Opinion 5/2021, para. 35.

15 The EU-funded project started on 1 September 2016 and ended on 31 August 2019. See Intelligent Portable Border Control System, https://cordis.europa.eu/project/id/700626.

The AI Act has not prohibited AI systems, such as lie detectors, from being used by competent public authorities, including at the EU level, to assess risks posed by people who intend to enter or have entered the territory of a Member State. Instead, such systems are classified as high risk,[16] which implies that they are subject to stricter rules, including prior fundamental risk assessment, continuous monitoring of their development and use, and an individual right of explanation.

Moreover, some of these safeguards for high-risk systems have exceptions in the migration context. In particular, the requirement that human supervision must involve separate verification by at least two natural persons does not apply to AI systems used for law enforcement and migration, border, or asylum management, 'where Union or national law considers the application of this safeguard to be disproportionate'.[17]

Treating individuals suspected of having committed a crime in the same category as migrants or asylum seekers is another challenge resulting from the worrying tendency of EU legislators – favoured by the interoperability of large-scale IT systems and the deployment of AI tools – to blur the distinction between the different policy areas of asylum, migration, police cooperation, internal security, and criminal justice.[18]

The Role of Data Protection Principles

In this context, data protection principles and rules should play a critical role in helping navigate the pitfalls of AI and preserve the dignity of all those in vulnerable situations.

For instance, on 30 September 2019, the EDPS issued a temporary ban on the production of social media monitoring (SMM) reports by the European Asylum Support Office (EASO) – now known as the European Union Agency for Asylum (EUAA). EASO was using SMM reports to provide EASO management and relevant stakeholders (Member States, European institutions and EU agencies, UNHCR, the IGC, Interpol, and the International Organization for Migration) with news on the latest shifts in asylum and migration routes and smuggling offers, as well as an overview of conversations in the social media community relating to key issues, such as flight, human trafficking, and other asylum systems and processes. EASO was doing this without the necessary legal basis.

16 Annex III to the AI Act, point 7 (b).

17 Article 14(5) AI Act.

18 On 8 January 2025, the EDPS reprimanded Frontex, the European Border and Coast Guard Agency, for not complying with Regulation (EU) 2019/1896 (Frontex Regulation), when transmitting personal data of suspects of cross-border crimes to Europol, the EU's agency for law enforcement cooperation.

Social media monitoring tools in general raise a number of serious data protection concerns. In the EASO case, these included a chilling effect – the tendency for users to self-censor their online content if they thought it might be monitored - high risks posed to the fundamental rights of the individuals and groups monitored, a lack of fairness and transparency involved in processing this data, and the vast number of social media users implicated. Given these concerns, EU institutions, bodies, and agencies must not only have a specific legal basis for carrying out social media monitoring, which EASO did not have, but also complement such processing operations with robust additional safeguards.[19]

Among the principles which are particularly relevant in the context of migration monitoring, human oversight of automated decision-making[20] appears to be an essential safeguard that needs to be properly implemented. It reflects one of the core principles of the Vienna Manifesto on Digital Humanism, which proclaimed that "(d)ecisions with consequences that have the potential to affect individual or collective human rights must continue to be made by humans".

Human oversight needs to be effective and, to be so, requires monitoring and auditing of both the system and the operator, in light of their respective fallibility. Already in 2010, researchers showed how the use of automated fingerprint identification systems affected the decision-making of experts, who put more trust in the outputs from the machine even if they were not able to understand the decision-making process.[21] In this regard, the understanding of the outputs of AI systems, and the subsequent possibility of explaining such outputs, are key issues for the full compliance of the use of such systems with the principle of human intervention: "The adoption of (explainable AI) contributes to a future where AI should be defined not only by its technical capabilities, but also by humanity's collective responsibility to uphold human rights, ethics, and accountability".[22]

The human dimension in the context of the use of AI is all the more important in the humanitarian field: beyond the need to keep control over the

19 See the EDPS decision on a temporary ban on the production of social media monitoring reports by EASO, in the absence of a clear legal basis and considering the risks to individuals' fundamental rights and freedoms: Formal consultation on EASO's social media monitoring reports (case 2018-1083), https://www.edps.europa.eu/sites/default/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.

20 Article 22 of the GDPR enshrines the right of the data subject to obtain human intervention on the part of the controller, in the case of automated individual decision-making.

21 Matthew L. Smith, Merel E. Noorman, and Aaron K. Martin "Automating the public sector and organizing accountabilities," *Communications of the Association for Information Systems* 26, no. 1 (2010): 1. https://doi.org/10.17705/1CAIS.02601.

22 EDPS TechDispatch on Explainable Artificial Intelligence, 16 November 2023, https://www.edps.europa.eu/system/files/2023-11/23-11-16_techdispatch_xai_en.pdf.

machine, stakeholders cannot renounce – voluntarily or otherwise – human interaction and oversight: "(...) one thing that digital technologies cannot do (yet) is to provide the empathy inherent to respect for human dignity".[23]

Data Protection as a Compass Towards a Digital Humanism

The processing of personal data is central to the AI systems used in the context of humanitarian action, both as input data and as a result of their deployment, generating in turn more data.

For as much as the law can provide for permitted vs. banned uses of a certain technology, the law is not always sufficient to draw a clear line between right and wrong. There is a renewed importance of ethics in the AI context; ethical guidelines and codes of conduct may complement the law, but should not replace it. As Carl Miller already underlined in 2019:

> *moralising the tech giants is a distraction from what actually has to be done: reforming the moral architecture outside them (...) Refreshing our moral order for the digital age does not boil down to corporate social responsibility, or to shaming a specific industry into doing a specific thing. It's down to all the rest of us. We need to stop trying to turn private companies into something they're not, and start building a new moral, institutional and legal order to express the values, rights and standards that we hold into the digital realm.*[24]

The world of AI is controlled, as with many other areas in the digital realm, by a very limited number of large firms, the only ones with the ability to develop and deploy AI at scale. These companies make decisions with a crucial societal impact. AI should not only serve the interests of those who control it. In the same vein, AI should not lead to a form of voluntary servitude that shapes and standardises our gestures, our habits, and even our ways of thinking. Even more so, AI should not lead to a situation of dependency on technology, a situation where humanity would no longer be able to act on its own, as human competences would decline and be delegated to AI.

We must embark on a profound rethinking of the technology market structure and the accumulation of power that comes from it, as it has a direct impact on people's fundamental rights, including the right to privacy and data

23 Pierrick Devidal, "'Back to basics' with a digital twist: humanitarian principles and dilemmas in the digital age," 2 February 2023, https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/.

24 Carl Miller, "It's time to forcibly reform big tech," *Wired*, August 2019, https://www.wired.com/story/tech-reform-regulation/.

protection. EU legal interventions such as the Digital Markets Act,[25] Digital Services Act,[26] and the like, will certainly help. There are other similar initiatives beyond the EU, and they are already advancing the cause of protecting the rights of people. The legislation is of course necessary, but beyond the legislative frameworks, we need to have an ethical approach, and decide when and how AI systems may be used. As Floridi remarks:

> *(...) even in the EU, legislation is necessary but insufficient. It does not cover everything (nor should it), and agents should leverage digital ethics in order to assess and decide what role they wish to play in the infosphere, when regulations provide no simple or straightforward answer, when competing values and interests need to be balanced (or indeed when regulations provide no guidance) and when there is more that can be done over and above what the law strictly requires.*[27]

We must devise the trajectory for a future which can be just and fair to everyone. This trajectory must pass through privacy and data protection, conceived as fundamental guiding references. It is about a digital humanism, which of course cannot contemplate digital artefacts such as AI systems, possibly deployed on a large scale, which run counter to human rights. AI must be shaped in accordance with human values and needs.[28]

Ultimately, these rights are rooted in the overarching principle of human dignity, as enshrined in Article 1 of the Universal Declaration of Human Rights.[29] This principle (dignity) is also at the root of the fundamental rights to privacy and to the protection of personal data.

One particular area of attention is the threat to democracy represented by misinformed and disinformed news, images, and video. The creation and circulation of this content are increasingly facilitated by generative AI systems. The challenge associated with discerning what is true from what is false is already a matter of concern. But the possible use of such manipulated

25 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), OJ L 265, 12.10.2022, 1–66.

26 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), OJ L 277, 27.10.2022, 1–102.

27 Luciano Floridi, "Soft Ethics and the Governance of the Digital," *Philos. Technol.* 31, no. 1–8 (2018).

28 Vienna Manifesto on Digital Humanism, https://caiml.org/dighum/dighum-manifesto/.

29 Universal Declaration of Human Rights, Article 1: "All human beings are born free and equal in dignity and rights," https://www.un.org/en/about-us/universal-declaration-of-human-rights.

content for political gain and propaganda is even more concerning and could tear apart trust in societies, thus undermining the very pillars of democracy. Discussions on how deepfakes and disinformation will play out in elections and the democratic process are increasing in intensity, as well as the risk of the weaponisation of information in the context of humanitarian operations.[30]

Conclusion

More than ever, the data protection community from all over the world has a crucial role to play in the context of the implementation of AI: as long as personal data is used to fuel the development, training, and testing of AI systems, the data protection framework is often the first line of defence for other fundamental rights. This is particularly true in the context of humanitarian action, where individuals face threats to their lives.

It does not mean that it will be an easy task. In such extreme situations, the asymmetry of power between those who are in need of protection and those who can give them such support – either humanitarian organisations or other public or private entities – may lead them to renounce the enjoyment of their fundamental rights.

AI does not happen to us; choices made by people determine its future.[31]

30 International Review of the Red Cross, "Q&A: Humanitarian operations, the spread of harmful information and data protection," March 2021, https://international-review.icrc.org/articles/humanitarian-operations-harmful-information-data-protection-913.

31 AI Action Summit, International AI Safety Report, January 2025, https://assets.publishing.service.gov.uk/media/679a0c48a77d250007d313ee/International_AI_Safety_Report_2025_accessible_f.pdf.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

INDEX