

HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION

CO-EDITORS: CHRISTOPHER KUNER AND MASSIMO MARELLI

SECOND EDITION



BRUSSELS
PRIVACY
HUB



ICRC

HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION

CO-EDITORS: CHRISTOPHER KUNER AND MASSIMO MARELLI

SECOND EDITION

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	10
------------------------	----

FOREWORD	11
----------------	----

GLOSSARY OF DEFINED TERMS AND ABBREVIATIONS	12
---	----

PART I – GENERAL CONSIDERATIONS

1. INTRODUCTION	19
-----------------------	----

1.1 Background	20
1.2 Objective	21
1.3 Structure and approach	25
1.4 Target audience	25

2. BASIC PRINCIPLES OF DATA PROTECTION	27
--	----

2.1 Introduction	28
2.2 Basic data protection concepts	31
2.3 Aggregate, Pseudonymized and Anonymized data sets	33
2.4 Applicable law and International Organizations	34
2.5 Data Processing principles	35
2.5.1 The principle of the fairness and lawfulness of Processing	35
2.5.2 The purpose limitation principle	36
2.5.3 The principle of proportionality	36
2.5.4 The principle of data minimization	38
2.5.5 The principle of data quality	39
2.6 Special data Processing situations	39
2.6.1 Health purposes	39
2.6.2 Administrative activities	41
2.6.3 Further Processing	41
2.7 Data retention	43
2.8 Data security and Processing security	43
2.8.1 Introduction	43
2.8.2 Physical security	45
2.8.3 IT security	46
2.8.4 Duty of discretion and staff conduct	47
2.8.5 Contingency planning	48
2.8.6 Destruction methods	48
2.8.7 Other measures	49
2.9 The principle of accountability	49
2.10 Information	50
2.10.1 Data collected from the Data Subject	50

2.10.2	Information notices.....	51
2.10.3	Data not collected from the Data Subject.....	52
2.11	Rights of Data Subjects	53
2.11.1	Introduction.....	53
2.11.2	Access	53
2.11.3	Correction.....	55
2.11.4	Right to erasure	55
2.11.5	Right to object.....	56
2.12	Data sharing and International Data Sharing	57
3.	LEGAL BASES FOR PERSONAL DATA PROCESSING	59
3.1	Introduction	60
3.2	Consent.....	61
3.2.1	Unambiguous.....	62
3.2.2	Timing.....	62
3.2.3	Validity	62
3.2.4	Vulnerability	62
3.2.5	Children	63
3.2.6	Informed.....	64
3.2.7	Documented.....	65
3.2.8	Withholding/withdrawing Consent	65
3.3	Vital interest	66
3.4	Important grounds of public interest	67
3.5	Legitimate interest	68
3.6	Performance of a contract	70
3.7	Compliance with a legal obligation	70
4.	INTERNATIONAL DATA SHARING.....	73
4.1	Introduction	74
4.2	Basic rules for International Data Sharing	76
4.3	Providing a legal basis for International Data Sharing	76
4.3.1	Introduction	76
4.3.2	Legal bases for International Data Sharing.....	77
4.4	Mitigating the risks to the individual	77
4.4.1	Appropriate safeguards/Contractual clauses.....	78
4.4.2	Accountability.....	79
4.5	Data Controller/Data Processor relationship	80
4.6	The disclosure of Personal Data to authorities	80
5.	DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)	83
5.1	Introduction	84
5.2	The DPIA process	86
5.2.1	Is a DPIA necessary?	86
5.2.2	The DPIA team	86
5.2.3	Describing the Processing of Personal Data	87

5.2.4	Consulting stakeholders.....	87
5.2.5	Identify risks	87
5.2.6	Assess the risks.....	88
5.2.7	Identify solutions.....	88
5.2.8	Propose recommendations	88
5.2.9	Implement the agreed recommendations	88
5.2.10	Provide expert review and/or audit of the DPIA.....	89
5.2.11	Update the DPIA if there are changes in the project.....	89

PART II – SPECIFIC PROCESSING SITUATIONS AND TECHNOLOGIES

6.	DATA ANALYTICS AND BIG DATA	91
6.1	Introduction	92
6.2	Application of basic data protection principles	97
6.2.1	Purpose limitation and Further Processing	98
6.2.2	Legal bases for Personal Data Processing	100
6.2.3	Fair and lawful Processing.....	102
6.2.4	Data minimization.....	103
6.2.5	Data security	104
6.3	Rights of Data Subjects	105
6.4	Data sharing	106
6.5	International Data Sharing	106
6.6	Data Controller/Data Processor relationship	107
6.7	Data Protection Impact Assessments	108
7.	DRONES/UAVS AND REMOTE SENSING	111
7.1	Introduction	112
7.2	Application of basic data protection principles	115
7.2.1	Legal bases for Personal Data Processing	115
7.2.2	Transparency/Information	119
7.2.3	Purpose limitation and Further Processing	119
7.2.4	Data minimization.....	120
7.2.5	Data retention.....	120
7.2.6	Data security	121
7.3	Rights of Data Subjects	121
7.4	Data sharing	122
7.5	International Data Sharing	123
7.6	Data Controller/Data Processor relationship	124
7.7	Data Protection Impact Assessments	124
8.	BIOMETRICS	127
8.1	Introduction	128
8.2	Application of basic data protection principles	130
8.2.1	Legal bases for Personal Data Processing	132
8.2.2	Fair and lawful Processing.....	135

8.2.3	Purpose limitation and Further Processing	135
8.2.4	Data minimization.	137
8.2.5	Data retention	137
8.2.6	Data security	138
8.3	Rights of Data Subjects	138
8.4	Data sharing	138
8.5	International Data Sharing	139
8.6	Data Controller/Data Processor relationship	139
8.7	Data Protection Impact Assessments	140
9.	CASH TRANSFER PROGRAMMING	143
9.1	Introduction	144
9.2	Application of basic data protection principles	148
9.3	Basic principles of data protection	149
9.3.1	Legal bases for Personal Data Processing	150
9.3.2	Purpose limitation and Further Processing	152
9.3.3	Data minimization.	153
9.3.4	Data retention	154
9.3.5	Data security	155
9.4	Rights of Data Subjects	156
9.5	Data sharing	156
9.6	International Data Sharing	157
9.7	Data Controller/Data Processor relationship	157
9.8	Data Protection Impact Assessments	158
10.	CLOUD SERVICES	161
10.1	Introduction	162
10.2	Responsibility and accountability in the cloud	164
10.3	Application of basic data protection principles	165
10.3.1	Legal bases for Personal Data Processing	165
10.3.2	Fair and lawful Processing.	167
10.3.3	Purpose limitation and Further Processing	167
10.3.4	Transparency	168
10.3.5	Data retention	168
10.4	Data security.	169
10.4.1	Data in transit protection.	173
10.4.2	Asset Protection	173
10.4.2.1	Physical location	173
10.4.2.2	Data centre security	174
10.4.2.3	Data at rest security	174
10.4.2.4	Data sanitization.	174
10.4.2.5	Equipment disposal.	174
10.4.2.6	Availability	174
10.4.3	Separation between users	175

10.4.4	Governance	175
10.4.5	Operational security	175
10.4.6	Personnel	176
10.4.7	Development	176
10.4.8	Supply chain	176
10.4.9	User management	176
10.4.10	Identity and authentication	177
10.4.11	External interfaces	177
10.4.12	Service administration	177
10.4.13	Audits	177
10.4.14	Service usage	177
10.5	Rights of Data Subjects	178
10.6	International Data Sharing	178
10.7	Data Controller/Data Processor relationship	178
10.8	Data Protection Impact Assessments	179
10.9	Privileges and immunities and the cloud	179
10.9.1	Legal measures	180
10.9.2	Organizational measures	180
10.9.3	Technical measures	181

11. MOBILE MESSAGING APPS 183

11.1	Introduction	184
11.1.1	Mobile messaging apps in Humanitarian Action	186
11.2	Application of basic data protection principles	187
11.2.1	Processing of Personal Data through mobile messaging apps .	187
11.2.1.1	<i>Potential threats</i>	188
11.2.2	What kind of data do messaging apps collect or store?	189
11.2.3	How could other parties access data shared on messaging apps?	192
11.2.4	Messaging app features related to privacy and security	194
11.2.4.1	<i>Anonymity permitted/no requirement for authenticated identity</i>	194
11.2.4.2	<i>No retention of message content</i>	195
11.2.4.3	<i>End-to-end encryption</i>	195
11.2.4.4	<i>User ownership of data</i>	195
11.2.4.5	<i>No or minimal retention of metadata</i>	195
11.2.4.6	<i>Messaging-app code is open source</i>	196
11.2.4.7	<i>Company vets disclosure requests from law enforcement</i>	196
11.2.4.8	<i>Limited Personal Data sharing with Third Parties</i>	196
11.2.4.9	<i>Restricting access through the device's operating system, software or specific security patches</i>	197
11.2.5	Processing of Personal Data collected through mobile messaging apps	197
11.3	Legal bases for Personal Data Processing	198

11.4	Data retention	198
11.5	Data Subject Rights to rectification and deletion	199
11.6	Data Minimization	199
11.7	Purpose limitation and Further Processing	200
11.8	Managing, analysing and verifying data	201
11.9	Data protection by design	202
11.10	International Data Sharing	202
12.	DIGITAL IDENTITY	205
12.1	Introduction	206
12.1.1	Authentication, identification and verification: Who are you and how can you prove it?	208
12.1.2	Digital Identity	209
12.1.3	System design and governance.	210
12.1.4	Digital Identity in the humanitarian sector: Possible scenarios	211
12.1.5	Digital Identity as foundational identity	212
12.2	Data Protection Impact Assessments	214
12.3	Data Protection by Design and by Default	214
12.4	Data Controller/Data Processor relationship.	215
12.5	Rights of Data Subjects	216
12.5.1	Right of access	217
12.5.2	Rights to rectification and erasure	218
12.6	Application of basic data protection principles	218
12.6.1	Legal bases for Personal Data Processing	218
12.6.2	Purpose limitation and Further Processing	219
12.6.3	Proportionality	219
12.6.4	Data minimization.	220
12.6.5	Data security	220
12.6.6	Data retention	221
12.7	International data sharing	221
13.	SOCIAL MEDIA	223
13.1	Introduction	224
13.1.1	Social media in the humanitarian sector.	224
13.1.2	Social media and data	226
13.1.2.1	What data are generated on social media and how?	226
13.1.2.2	What data can be shared with third parties?	228
13.1.2.3	What data can law enforcement and government authorities obtain?	229
13.2	Data Protection Impact Assessments	230
13.3	Ethical issues and other challenges	232
13.4	Data Controller/Data Processor relationship.	233
13.5	Basic data protection principles	234

13.5.1	Legal bases for Personal Data Processing	234
13.5.2	Information	235
13.5.3	Data retention	236
13.5.4	Data security	237
13.6	International data sharing	237

14. BLOCKCHAIN..... 239

14.1	Introduction	240
14.1.1	What is Blockchain?	240
14.1.2	Types of Blockchain	242
14.1.3	Blockchain in practice	244
14.1.4	Humanitarian use cases	246
14.2	Data Protection Impact Assessments	248
14.3	Data Protection by Design and by Default	249
14.4	Data Controller/Data Processor relationship	250
14.5	Basic data protection principles	252
14.5.1	Data minimization	252
14.5.2	Data retention	253
14.5.3	Proportionality	253
14.5.4	Data security	254
14.6	Rights of Data Subjects	255
14.6.1	Right of access	255
14.6.2	Right to rectification	255
14.6.3	Right to erasure	256
14.6.4	Restrictions of Data Subjects' rights	257
14.7	International data sharing	257
	Annex: Decision-making framework for Blockchain in humanitarian action	258

15. CONNECTIVITY AS AID 263

15.1	Introduction	264
15.1.1	Overview of connectivity as aid interventions	264
15.1.2	Operational context	265
15.1.3	Multiple stakeholders and partnerships	266
15.2	Data Protection Impact Assessments	268
15.3	Data Controller/Data Processor relationship	269
15.4	Basic data protection principles	270
15.4.1	Legal bases for Personal Data Processing	270
15.4.2	Data security	271
15.4.3	Data retention	272
15.4.4	Information	273
15.5	International data sharing	273

16. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.	275
16.1 Introduction	276
16.1.1 What are Artificial Intelligence and Machine Learning?	276
16.1.2 How do Artificial Intelligence and Machine Learning work? . .	277
16.1.3 Artificial Intelligence in the humanitarian sector.	279
16.1.4 Challenges and risks of using Artificial Intelligence	280
16.2 Data Protection Impact Assessment	281
16.3 Application of basic data protection principles	282
16.3.1 Purpose limitation and Further Processing	282
16.3.2 Fair and lawful Processing.	283
16.3.2.1 <i>Lawfulness</i>	283
16.3.2.2 <i>Fairness v. bias</i>	285
16.3.2.3 <i>Transparency</i>	286
16.3.3 Data minimization.	287
16.3.4 Data retention	288
16.3.5 Data security	289
16.4 Rights of Data Subjects	290
16.4.1 Right to be informed	290
16.4.2 Right to erasure	291
16.4.3 Rights in relation to automated decision-making.	291
16.5 Data Controller/Data Processor relationship.	293
16.5.1 Accountability.	293
16.5.2 Liability.	293
16.6 International Data Sharing	294
16.7 Data Protection by Design and by Default	294
16.8 Ethical issues and challenges.	296
 APPENDIX I. TEMPLATE FOR A DPIA REPORT	 299
 APPENDIX II. WORKSHOP PARTICIPANTS	 305

ACKNOWLEDGEMENTS

This Handbook is a joint publication of the Brussels Privacy Hub, an academic research centre of the Vrije Universiteit Brussel (Free University of Brussels or VUB) in Brussels, Belgium, and the Data Protection Office of the International Committee of the Red Cross (ICRC) in Geneva, Switzerland.

Christopher Kuner, VUB, and Massimo Marelli, ICRC, co-edited the Handbook.

The advisory board and drafting team comprised:

- Christopher Kuner, Júlia Zomignani Barboza, and Lina Jasmontaite, VUB
- Massimo Marelli, Vincent Graf Narbel, Sarah Dwidar, Luca Bettoni, Pierre Apraxine and Romain Bircher, ICRC
- Catherine Lennman, Swiss Data Protection Authority
- Claire-Agnes Marnier, Olivier Matter and Petra Candellier, European Data Protection Supervisor
- Alexander Beck, Office of the United Nations High Commissioner for Refugees (UNHCR)
- Christina Vasala Kokkinaki, International Organization for Migration (IOM)
- Lucie Laplante and James De France, International Federation of Red Cross and Red Crescent Societies (IFRC)
- Stuart Campo, United Nations Office for the Coordination of Humanitarian Affairs
- Nathaniel Raymond, Yale University
- Alexandrine Pirlot de Corbion, Privacy International
- Marine Revel, French-speaking Association of Personal Data Protection Authorities
- Carmela Troncoso, Swiss Federal Institute of Technology in Lausanne
- Mary Nunn, Médecins Sans Frontières
- Awa Ndiaye and Anna Thiam, Senegalese Data Protection Authority.

The authors express their gratitude to ICT Legal Consulting for permission to use the material on cloud security: <https://www.ictlegalconsulting.com/?lang=en> and to Trilateral Research: <http://trilateralresearch.com/> for permission to use the material on Data Protection Impact Assessments.

Where a chapter of this Handbook relies on specific contributions made by third parties, this is also acknowledged in a footnote in the relevant chapter.

FOREWORD

Jean-Philippe Walter, Data Protection Commissioner, Council of Europe, and Member of the ICRC Data Protection Independent Control Commission

It is a pleasure to introduce the Handbook on Data Protection in Humanitarian Action, which is the result of a very fruitful collaboration between the International Committee of the Red Cross (ICRC) and the Brussels Privacy Hub (BPH).

Personal data protection is of fundamental importance for humanitarian organizations as it is an integral part of protecting the life, integrity and dignity of their beneficiaries.

In 2015, the 37th International Conference of Data Protection and Privacy Commissioners adopted the Resolution on Privacy and International Humanitarian Action. One of resolution's aims was to meet the demand among humanitarian actors for cooperation to develop guidance on data protection. A working group was set up and became involved in the Data Protection in Humanitarian Action project, run jointly by the BPH and the ICRC, whose objectives were to explore the relationship between data protection laws and Humanitarian Action, to understand the impact of new technologies on data protection in the humanitarian sector and to formulate appropriate guidance.

The project brought together humanitarian organizations, data protection authorities and technology experts in a series of workshops covering a range of topics, including data analytics, drones, biometrics, cash transfer programming, cloud-based computing and messaging apps, all of which have become increasingly important in the humanitarian sector.

The Handbook is one of the outputs of this project; it will be a useful tool to raise awareness and assist humanitarian organizations in complying with personal data protection standards. It also addresses the need for specific guidance on the interpretation of data protection principles as applicable to humanitarian action, especially when new technologies are employed. I believe the Handbook will prove helpful to humanitarian actors, data protection authorities and private companies alike. It clearly demonstrates that data protection legislation does not prohibit the collection and sharing of personal data, but rather provides the framework in which personal data can be used in the knowledge and confidence that individuals' right to privacy is respected.

Jean-Philippe Walter is former Deputy Swiss Federal Data Protection and Information Commissioner and has also been president of the French-speaking Association of Personal Data Protection Authorities and coordinator of the International Conference of Data Protection and Privacy Commissioners (now Global Privacy Assembly) Working Group on the Resolution on Privacy and International Humanitarian Action.

GLOSSARY OF DEFINED TERMS AND ABBREVIATIONS

Anonymization encompasses techniques that can be used to ensure that data sets containing Personal Data are fully and irreversibly anonymized so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.

Artificial Intelligence refers to “[a] set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being.”¹ In its current form, it aims to allow technology developers “to entrust a machine with complex tasks previously delegated to a human.”²

Biometrics or biometric recognition means the automated recognition of individuals based on their biological and behavioural characteristics.

Blockchain is “in essence an append-only decentralized database that is maintained by a consensus algorithm and stored on multiple nodes (computers).”³

Cash Transfer Programming, cash and voucher assistance, cash-based interventions and cash-based assistance are terms in the humanitarian sector to describe the delivery of humanitarian aid in the form of vouchers or cash.

CERT – Computer Emergency Response Team

CISO – Chief Information Security Officer

Cloud Services most commonly refers to “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.”⁴

Consent means the freely-given, specific and informed indication of a Data Subject’s wishes by which the Data Subject signifies agreement to Personal Data relating to him or her being processed.

CSIRT – Computer Security Incident Response Team

CSO – Chief Security Officer

CTO – Chief Technology Officer

1 Council of Europe (CoE), Glossary on Artificial Intelligence: <https://www.coe.int/en/web/artificial-intelligence/glossary>.

2 CoE, Glossary on Artificial Intelligence.

3 Finck, *Blockchains and Data Protection in the European Union*, 4(1) *European Data Protection Law Review* (2018), p. 17: <https://doi.org/10.21552/edpl/2018/1/6>.

4 US NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

Data Analytics denotes the practice of combining very large volumes of diversely sourced information (Big Data) and analysing them, using sophisticated algorithms to inform decisions.

Data Breach means the unauthorized modification, copying, unlawful destruction, accidental loss, improper disclosure or undue transfer of, or tampering with, Personal Data.

Data Controller means the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Data Processor means the person or organization who processes Personal Data on behalf of the Data Controller.

Data Protection Impact Assessment or DPIA means an assessment that identifies, evaluates and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.

Data Subject means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Digital Identity refers to “a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions.”⁵

DPO in the context of this Handbook means a Humanitarian Organization’s internal data protection office or data protection officer.

Drones are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS).

Further Processing means additional Processing of Personal Data that goes beyond the purposes originally specified at the time the data were collected.

Health Data means data related to the physical or mental health of an individual, which reveal information about his/her health status.

Humanitarian Action means any activity undertaken on an impartial basis to carry out assistance, relief and protection operations in response to a Humanitarian Emergency. Humanitarian Action may include “humanitarian assistance”, “humanitarian aid” and “protection”.

Humanitarian Emergency means an event or series of events (in particular arising out of armed conflicts or natural disasters) that poses a critical threat to the health, safety, security or wellbeing of a community or other large group of people, usually over a wide area.

5 GSMA, World Bank Group, & Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, p. 11: <https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/>.

Humanitarian Organization means an organization that provides aid to alleviate human suffering, and/or protects life and health, and upholds human dignity during Humanitarian Emergencies in accordance with its mandate and/or mission.

IaaS stands for Infrastructure as a Service.

International Data Sharing includes any act of transferring or making Personal Data accessible outside the country or International Organization where they were originally collected or processed, including both to a different entity within the same Humanitarian Organization or to a Third Party, via electronic means, the internet, or other means.

International Organization means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Know Your Customer (KYC) is a process enabling businesses to check the identity of their customers in order to comply with regulations and legislation on money laundering and corruption.⁶

Machine Learning is a specific form of Artificial Intelligence that can be defined as the study of algorithms that improve their performance when completing a certain task with experience in the form of machine-readable data.

PaaS – Platform as a Service

Personal Data means any information relating to an identified or identifiable natural person.

Processing means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination or erasure.

Pseudonymization, as distinct from Anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

SaaS – Software as a Service

Sensitive Data means Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels

⁶ PWC, Know Your Customer: Quick Reference Guide: <http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html>.

of sensitivity. Given the specific situations in which Humanitarian Organizations work and the possibility that some data elements could give rise to discrimination, setting out a definitive list of Sensitive Data categories in Humanitarian Action is not meaningful. Sensitivity of data as well as appropriate safeguards (e.g. technical and organizational security measures) have to be considered on a case-by-case basis.

SLA – A service-level agreement is an official commitment between a service provider and a client, particularly for the provision of reliable telecommunications and internet services.

Sought Person is a person unaccounted for, for whom a tracing operation has been launched.

Sub-Processor is a person or organization that is engaged by a Data Processor to process Personal Data on its behalf.

Third Party is any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller and the Data Processor.

TLS – Transport Layer Security is a cryptographic protocol to provide privacy and data integrity between a client and a server over an internet connection.

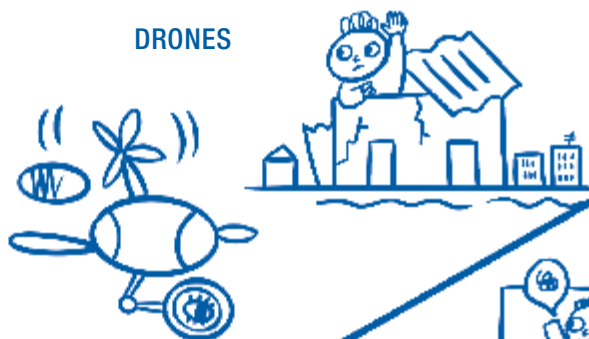


ICRC



BRUSSELS
PRIVACY
HUB

DRONES



SOCIAL MEDIA



© ICRG
SUPPLIES
AVAILABLE!



BLOCKCHAIN



ARTIFICIAL
INTELLIGENCE

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Protecting individuals' Personal Data is an integral part of protecting their life, integrity and dignity. This is why Personal Data protection is of fundamental importance for Humanitarian Organizations.

In suggesting how data protection principles should be applied by Humanitarian Organizations, this Handbook builds on existing guidelines, working procedures and practices that have been established in Humanitarian Action in the most volatile environments and for the benefit of the most vulnerable victims of armed conflicts, other situations of violence, natural disasters, pandemics and other Humanitarian Emergencies (together “Humanitarian Emergencies”). Some of these guidelines, procedures and practices pre-date the advent and development of data protection laws, but they all are based on the principle of human dignity and the same concept of protection which underpin data protection law. These guidelines have been set out, notably, in the Professional Standards for Protection Work.⁷



A motorcyclist rides past war-damaged buildings in the town of al-Bab, Syria, March 2017.

⁷ ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 2nd ed., Geneva 2013: <https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights>, all internet references accessed in March 2020.

In recent years, the development of new technologies allowing for easier and faster Processing of ever-increasing quantities of Personal Data in an inter-connected world has given rise to concerns about the possible intrusion into the private sphere of individuals. Regulatory efforts around the globe are ongoing to respond to these concerns.

This Handbook is published as part of the Brussels Privacy Hub and ICRC's Data Protection in Humanitarian Action project, which was organized jointly by the Brussels Privacy Hub, an academic research centre of the Vrije Universiteit Brussel (VUB) in Brussels, Belgium, and the ICRC Data Protection Office in Geneva, Switzerland. The content of the Handbook was developed in a series of workshops held in Brussels and Geneva in 2015–2016, with representatives from Humanitarian Organizations (including humanitarian practitioners), data protection authorities, academics, non-governmental organizations, researchers and other experts on specific topics. They came together to address questions of common concern in the application of data protection in Humanitarian Action, particularly in the context of new technologies. The individuals who participated in the various workshops are listed in Appendix II.

1.2 OBJECTIVE

This Handbook aims to further the discussion launched by the International Conference of Data Protection and Privacy Commissioners' (ICDPPC's) Resolution on Privacy and International Humanitarian Action⁸ adopted in Amsterdam in 2015. It is not intended to replace compliance with applicable legal norms, or with data protection rules, policies and procedures that a particular organization may have adopted. Rather, the Handbook seeks to raise awareness and assist Humanitarian Organizations in ensuring that they comply with Personal Data protection standards in carrying out humanitarian activities, by providing specific guidance on the interpretation of data protection principles in the context of Humanitarian Action, particularly when new technologies are employed.

This Handbook is designed to assist in the integration of data protection principles and rights in the humanitarian environment. It does not, however, replace or provide advice in relation to the application of domestic legislation on data protection, where this is applicable to a Humanitarian Organization not benefitting from the privileges and immunities generally associated with an International Organization.

⁸ International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015: https://edps.europa.eu/sites/edp/files/publication/15-10-27_resolution_privacy_humanitarian_action_en.pdf.

Compliance with Personal Data protection standards requires taking into account the specific scope and purpose of humanitarian activities to provide for the urgent and basic needs of vulnerable individuals. Data protection and Humanitarian Action should be seen as compatible, complementary to, and supporting each other. Thus, data protection should not be seen as hampering the work of Humanitarian Organizations; on the contrary, it should be of service to their work. Equally, data protection principles should never be interpreted in a way that hampers essential humanitarian work, and should always be interpreted in a way that furthers the ultimate objective of Humanitarian Action, namely safeguarding the life, integrity and dignity of victims of Humanitarian Emergencies.

The recommendations and guidelines contained in this Handbook are based on some of the most important international instruments dealing with data protection, in particular the following:

- UN General Assembly Resolution 45/95 of 14 December 1990⁹ adopting the *Guidelines for the Regulation of Computerized Personal Data Files*,¹⁰ which includes the humanitarian clause calling for particular care and flexibility when applying data protection principles in the humanitarian sector
- the UN Principles on Personal Data Protection and Privacy, adopted by the UN High-Level Committee on Management (HLCM) at its 36th Session on 11 October 2018¹¹
- the *International Standards on the Protection of Personal Data and Privacy* (The Madrid Resolution) adopted by the ICDPPC in Madrid in 2009¹²
- *The OECD Privacy Framework* (2013)¹³
- the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108),¹⁴ including Protocol CETS No. 223 amending the Convention (now known as Convention 108+).¹⁵

⁹ UN General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95 14 December 1990.

¹⁰ UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990: <http://www.refworld.org/docid/3ddcafaac.html>.

¹¹ UN High-Level Committee on Management (HLCM), UN Principles on Personal Data Protection and Privacy, 18 December 2018: <https://www.unsystem.org/personal-data-protection-and-privacy-principles>.

¹² International Conference on Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy*: http://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10.

¹³ *The OECD Privacy Framework*: <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

¹⁴ CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>.

¹⁵ CoE, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 10 October 2018, CETS 223: <https://rm.coe.int/16808ac918>.

Other important standards have also been taken into account, in particular:

- recent regulatory developments, insofar as they reflect further development of data protection concepts and principles in light of their application over the years and the challenges generated by new technologies (this includes the updating of Convention 108, as well as the EU General Data Protection Regulation 2016/679 (GDPR))¹⁶
- the Resolution on Data Protection and Major Natural Disasters¹⁷ adopted by the ICDPPC in Mexico City in 2011
- the Resolution on Privacy and International Humanitarian Action adopted by the ICDPPC in Amsterdam in 2015¹⁸
- the ICRC *Rules on Personal Data Protection* (2015)¹⁹
- the ICRC *Professional Standards for Protection Work* (2013)²⁰
- the UNHCR *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015)²¹
- the IOM *Data Protection Manual* (2010).²²

This Handbook provides recommended minimum standards for the Processing of Personal Data. Humanitarian Organizations may provide for stricter data protection requirements, should they deem it appropriate or be subject to stricter laws at the domestic or regional level.

¹⁶ EU Regulation 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 (EU General Data Protection Regulation), [2016] OJ L119/1.

¹⁷ International Conference on Data Protection and Privacy Commissioners, Resolution on Data Protection and Major Natural Disasters: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf?mc_phishing_protection_id=28047-britehqdu81eaoar3q10.

¹⁸ International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf?mc_phishing_protection_id=28047-britehqdu81eaoar3q10.

¹⁹ ICRC, *Rules on Personal Data Protection*: <https://www.icrc.org/en/document/data-protection>.

²⁰ ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 2nd ed., Geneva, 2013): <https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights>.

²¹ UN High Commissioner for Refugees (UNHCR), *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (May 2015): <http://www.refworld.org/docid/55643c1d4.html>.

²² International Organization for Migration (IOM), *Data Protection Manual* (2010): <https://publications.iom.int/books/iom-data-protection-manual>.

A few important considerations should be highlighted from the outset:

- The right to privacy has long been recognized globally as a human right,²³ while the right to Personal Data protection is a relatively recent human right that is closely connected to the right to privacy and sets forth conditions for the Processing of data of an identified or identifiable individual. More than 100 specific data protection laws and norms have been adopted at national and regional levels in recent years,²⁴ and Personal Data protection as a fundamental right is gaining wider acceptance around the world. Accordingly, implementation of Personal Data protection standards, even where not a legal obligation given the privileges and immunities enjoyed by certain Humanitarian Organizations, should be a priority for all Humanitarian Organizations, considering that the main objective of their activities is to work for the safety and dignity of individuals.
- Some Humanitarian Organizations are International Organizations enjoying privileges and immunities and not subject to national legislation. Respect for privacy and data protection rules is nevertheless, in many cases, a prerequisite for them to receive Personal Data from other entities.
- The exceptional emergency circumstances in which Humanitarian Organizations operate create special challenges regarding data protection. Accordingly, particular care and flexibility is required when applying data protection principles in the humanitarian sector. This need is also reflected in many of the international instruments and standards mentioned above, which include stricter rules for the Processing of Sensitive Data.²⁵
- The lack of a uniform approach in data protection law to the Personal Data of deceased individuals means that Humanitarian Organizations should adopt their own policies on this matter (for example, by applying the rules applicable to the Personal Data of natural persons to the deceased, insofar as this makes sense). For organizations that do not enjoy immunity from jurisdiction, this question may be regulated by the applicable law.
- The focus of this Handbook is on Personal Data protection, and the application of this area of law to Humanitarian Action. Yet, in armed conflicts and other situations of violence, many threats are collective rather than individual – a village, a community, a specific group of men and women may share the same threats. So just focusing on the proper management of Personal Data may not be sufficient. In some cases, Processing of non-Personal Data may raise specific threats at the collective level. In this respect, a number of initiatives in the humanitarian sector have been focusing on the implications of Processing data more generally for communities and referring, for example,

²³ See Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

²⁴ See United Nations Conference on Trade and Development (UNCTAD) report *Data Protection regulations and international data flows: Implications for trade and development* (2016): <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468>.

²⁵ See [Section 2.2: Basic data protection concepts](#).

to “demographically identifiable information”,²⁶ or “Community Identifiable Information”.²⁷

- Humanitarian Organizations process the Personal Data of different categories of individuals in Humanitarian Emergencies, such as data of beneficiaries and contacts involved in their activities, as well as data of staff and goods/service providers, or even data of donors. While the focus of this Handbook is the Processing of beneficiaries’ Personal Data, similar considerations apply to the handling of Personal Data of other categories of individuals.

1.3 STRUCTURE AND APPROACH

Part I of this Handbook applies generally to all types of Personal Data Processing. Part II deals with specific types of technologies and data Processing situations, and contains a more specific discussion of the relevant data protection issues. The specific Processing scenarios outlined in Part II should always be read with Part I in mind. Defined terms are capitalized throughout this Handbook; the definitions are contained in the Glossary at the beginning of the Handbook.

1.4 TARGET AUDIENCE

This Handbook is aimed at the staff of Humanitarian Organizations involved in Processing Personal Data for the humanitarian operations of their organization, particularly those in charge of advising on and applying data protection standards. It may also prove useful to other parties involved in Humanitarian Action or data protection, such as data protection authorities, private companies and any others involved in these activities.

²⁶ See The Signal Code – A Human Rights Approach to Information During Crisis: <https://signalcode.org/>.

²⁷ See Humanitarian Data Exchange Initiative: <https://data.humdata.org/about/terms>.

CHAPTER 2

BASIC PRINCIPLES OF DATA PROTECTION

2.1 INTRODUCTION

Humanitarian Organizations collect and process the Personal Data of individuals affected by Humanitarian Emergencies in order to perform humanitarian activities. Working primarily in Humanitarian Emergencies, they operate in situations where the rule of law may not be fully in force. In such situations, there may be limited, if any, access to justice and respect of the international human rights framework. In addition, Personal Data protection legislation may be embryonic or non-existent, or not entirely enforceable.

An individual's right to Personal Data protection is not an absolute right. It should be considered in relation to the overall objective of protecting human dignity, and be balanced with other fundamental rights and freedoms, in accordance with the principle of proportionality.²⁸

As the activities of Humanitarian Organizations are carried out primarily in Humanitarian Emergencies, they operate in situations where the protection of the Personal Data of beneficiaries and staff is often necessary to safeguard their



Walungu, South Kivu province, Democratic Republic of the Congo. The ICRC provides food to 1,750 displaced and local households, December 2016.

28 The principle of proportionality in this context should not be confused with the principle of proportionality under international humanitarian law (IHL). The principle of proportionality as discussed here requires that Humanitarian Organizations take the least intrusive measures available when limiting the right of data protection and access to Personal Data in order to give effect to their mandate and to operate in emergencies.

security, lives and work. Accordingly, Personal Data protection and Humanitarian Action are complementary and reinforce each other. However, there may also be instances of friction where a balance between different rights and freedoms needs to be struck (e.g. between the freedom of expression and information and the right to data protection, or between the right to liberty and security of a person and the right to data protection). The human rights framework aims to ensure respect for all human rights and fundamental freedoms by balancing different rights and freedoms on a case-by-case basis. This approach often requires teleological interpretation of rights,²⁹ i.e. one that prioritizes the purposes the rights serve.

EXAMPLE:

Data protection law requires that individuals be given basic information about the Processing of their Personal Data. However, in a Humanitarian Emergency it is necessary to balance this right against other rights, and in particular the rights of all affected individuals. It would therefore not be necessary to inform all individuals of the conditions of data collection prior to receiving aid, if this would seriously hamper, delay or prevent the distribution of aid. Rather, the Humanitarian Organizations involved could provide such information in a less targeted and individualized way with public notices, or individually at a later stage.

Some Humanitarian Organizations with a mandate under international law need to rely on specific working procedures, in order to be in a position to fulfil their mandate. Under international law these mandates can justify derogations from the principles and rights recognized in Personal Data Processing.

For example, it may be necessary to balance, on the one hand, data protection rights with, on the other hand, the objective of ensuring the historical and humanitarian accountability of stakeholders in Humanitarian Emergencies. Indeed, in Humanitarian Emergencies, Humanitarian Organizations may be the only external entities present, and may be the only possibility for future generations to have an external account of history as well as to provide a voice to victims.³⁰ Furthermore, data from Humanitarian Organizations may also be needed to support the victims of armed conflicts and other situations of violence or their descendants, for example in documenting their identity and legal status, submitting claims of reparations, etc. Data retention by Humanitarian Organizations may be of fundamental importance particularly considering that in Humanitarian Emergencies few or no other records may be available.

²⁹ In line with the humanitarian clause in the UN Guidelines for the regulation of computerized personal data files adopted by General Assembly Resolution 45/95 of 14 December 1990.

³⁰ See ICRC *WWI prisoner archives join UNESCO Memory of the World*, 15 November 2007: <https://www.icrc.org/eng/resources/documents/feature/2007/wwi-feature-151107.htm>.

Confidentiality may also be of fundamental importance for some Humanitarian Organizations, as it may be an essential precondition for the ongoing viability of Humanitarian Action in volatile environments, to ensure acceptance by parties to a conflict and people involved in other situations of violence, proximity to people in need and the safety of their staff. This may have an impact, for example, on the extent to which Data Subject access rights may be exercised.³¹

The checklist below sets out the main points explained in detail in this Handbook, which should be considered when dealing with data protection, in relation to the purpose or purposes for which data are processed:

- Is there Processing of Personal Data?
- Are individuals likely to be identified by the data processed?
- Does the information require protection even if it is not considered to be Personal Data?
- Have (if applicable) local data protection and privacy laws been complied with?
- For what purpose are the data being collected and processed? Is the Processing strictly limited to this purpose? Does this purpose justify the interference with the privacy of the Data Subject?
- What is the legal basis for Processing? How will it be ensured that the data are processed fairly and lawfully?
- Is the Processing of Personal Data proportionate? Could the same purpose be achieved in a less intrusive way?
- Which parties are Data Controllers and Data Processors? What is the relationship between them?
- Are the data accurate and up to date?
- Will the smallest amount of data possible be collected and processed?
- How long will Personal Data be retained? How will it be ensured that data are only retained as long as necessary to achieve the purpose of the Processing?
- Have adequate security measures been implemented to protect the data?
- Has it been made clear to individuals who is accountable and responsible for the Processing of Personal Data?
- Has information been provided to individuals about how their Personal Data are processed and with whom they will be shared?
- Are procedures in place to ensure that Data Subjects can assert their rights with regard to the Processing of Personal Data?
- Will it be necessary to share data with Third Parties? Under what circumstances will Personal Data be shared with or made accessible to Third Parties? How will individuals be informed of this?

³¹ See ICRC *WWI prisoner archives join UNESCO Memory of the World*, 15 November 2007: <https://www.icrc.org/eng/resources/documents/feature/2007/ww1-feature-151107.htm>.

- Will Personal Data be made accessible outside the country where they were originally collected or processed? What is the legal basis for doing so?
- Have Data Protection Impact Assessments been prepared to identify, evaluate, and address the risks to Personal Data arising from a project, policy, programme or other initiative?

2.2 BASIC DATA PROTECTION CONCEPTS³²

Data protection law and practice limit the **Processing of Personal Data** of **Data Subjects**, in order to protect individuals' rights.

Processing is to be interpreted to mean any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, or erasure.

Personal Data means any information relating to an identified or identifiable natural person. A Data Subject is a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.

Some data protection laws include the additional category of **Sensitive Data** in the concept of Personal Data. For the purposes of the present Handbook, Sensitive Data means Personal Data, which if disclosed, may result in discrimination against or the repression of an individual. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific environments in which Humanitarian Organizations work and the possibility that various data elements may give rise to discrimination, setting out a definitive list of Sensitive Data categories for Humanitarian Action is not meaningful. For example, in some situations, a simple list of names may be very sensitive, if it puts the individuals on the list and/or their families at risk of persecution. Equally, in other situations, data collected to respond to Humanitarian Emergencies may need to include data that in a regular data protection context would be considered to be Sensitive Data and the Processing of such data would be, in principle, prohibited, but in the local culture and the specific circumstances may be relatively harmless. Therefore, it is necessary to consider the sensitivity of

³² The terms defined below are also given in the [Glossary](#) at the beginning of the Handbook.

data and the appropriate safeguards to protect Sensitive Data (e.g. technical and organizational security measures) on case-by-case basis.

It is important to remember that during Humanitarian Emergencies, Processing data can cause severe harm even when the data cannot be considered Personal Data. Humanitarian Organizations should therefore be prepared to apply the protections described in this Handbook to other types of data as well, when failing to do so in a particular case would create risks to individuals.

EXAMPLE:

A Humanitarian Organization inadvertently reveals the number of individuals in a stream of people who are fleeing a situation of armed violence and publishes online aerial imagery related to this. One of the armed actors involved in the violence, which is the reason people are fleeing, then uses this information to locate the displaced population and targets them with reprisals. The number of individuals in a group and the aerial imagery (subject to the resolution and other factors potentially making it possible to identify individuals) is not by itself Personal Data, but such data can be extremely sensitive in certain circumstances. The Humanitarian Organization should have protected this data and not revealed it.

It is also important to understand the distinction between **Data Controller** and **Data Processor**. A Data Controller is the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data, whereas a Data Processor is the person or organization who processes Personal Data on behalf of the Data Controller. Finally, a Third Party is any natural or legal person, public authority, agency or any body other than the Data Subject, the Data Controller or the Data Processor.

EXAMPLE:

An International Humanitarian Organization collects information about the identity of individuals in a Humanitarian Emergency in order to provide them with aid. In order to do this, it engages the services of a local NGO to help deliver the aid, which needs to use the identification information originally collected by the Humanitarian Organization. The two organizations sign a contract governing the use of the data, under which the International Humanitarian Organization has the power to direct how the NGO uses the data and the NGO commits to respect the data protection safeguards required by the Humanitarian Organization. The NGO also engages an IT consulting company in order to perform routine maintenance on its IT system in which the data are stored.

In the above situation, the International Humanitarian Organization, the NGO and the IT consulting company are Processing the Personal Data of the individuals, who are the Data Subjects. The International Humanitarian Organization is a Data Controller and the NGO is a Data Processor, while the IT consulting company is a Sub-Processor.

2.3 AGGREGATE, PSEUDONYMIZED AND ANONYMIZED DATA SETS

As mentioned above, the Processing of data that does not relate to individual persons such as aggregate and statistical data, or data that has otherwise been rendered anonymous in such a way that the Data Subject is no longer identifiable, is outside the scope of this Handbook.

Where aggregate data are derived from Personal Data, and could in certain circumstances pose risks to persons of concern, it is important to ensure that the Processing, sharing, and/or publication of such data cannot lead to the re-identification of individuals.³³

Although specific Consent from Data Subjects is not required for their Personal Data to be used in aggregate data sets or statistics, Humanitarian Organizations should ensure that such data Processing has another legitimate basis,³⁴ and does not expose individuals or groups to harm, or otherwise jeopardize their protection.

The Anonymization of Personal Data can help meet the protection and assistance needs of vulnerable individuals in a privacy-friendly way. The term “Anonymization” encompasses techniques that can be used to convert Personal Data into anonymized data. When anonymizing data, it is essential to ensure that data sets containing Personal Data are fully and irreversibly anonymized. Anonymization processes are challenging, especially where large data sets containing a wide range of Personal Data are concerned and may pose a greater risk of re-identification.³⁵

33 See UK Statistics Authority, *National Statistician’s Guidance: Confidentiality of Official Statistics*: <https://www.statisticsauthority.gov.uk/archive/national-statistician/ns-reports--reviews-and-guidance/national-statistician-s-guidance/confidentiality-of-official-statistics.pdf>.

34 See [Chapter 3: Legal bases for Personal Data Processing](#).

35 See UK Information Commissioner’s Office, *Anonymisation: managing data protection risk – code of practice*: <https://ico.org.uk/media/1061/anonymisation-code.pdf>; see also EU Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

“Pseudonymization”, as distinct from Anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. This may involve replacing the anagraphic³⁶ data in a data set with a number. Sharing registration/identification numbers instead of names is good practice, but does not amount to Anonymization.

Prior to sharing or publicising anonymized data, it is important to ensure that no Personal Data are included in the data set and that individuals cannot be re-identified. The term “re-identification” describes the process of turning allegedly anonymized data back into Personal Data through the use of data matching or similar techniques.³⁷ If the risk of re-identification is deemed to be reasonably likely, the information should be considered to be Personal Data and subject to all the principles and guidance set out in this Handbook. It can be very difficult to assess the risk of re-identification with absolute certainty.

Prior to sharing or publishing aggregate data, it is important to ensure that the data sets do not divulge the actual location of small, at risk groups, for example by mapping data such as country of origin, religion or specific vulnerabilities to the geographical coordinates of persons of concern.

2.4 APPLICABLE LAW AND INTERNATIONAL ORGANIZATIONS

Humanitarian Action involves a large number of actors, such as Humanitarian Organizations, local authorities and private entities. As far as Humanitarian Organizations are concerned, some of them are non-governmental organizations (NGOs) subject to the jurisdiction of the country in which they operate, while others are International Organizations with privileges and immunities allowing them to perform the mandate attributed them by the community of states under international law in full independence.

As far as NGOs are concerned, the rules for determining applicable data protection law depend on a number of different factual elements. This Handbook does not deal with issues of applicable law; any questions in this regard should be directed to the NGO’s legal department or data protection office (DPO).³⁸

³⁶ <https://en.wiktionary.org/wiki/anagraphic>.

³⁷ Note, “identified” does not necessarily mean “named”; it can be enough to be able to establish a reliable connection between particular data and a known individual.

³⁸ See [Section 1.2: Objective](#).

In addition to any law that the NGO may be subject to, Personal Data Processing is controlled by its own internal data protection policy or rules, any contractual commitments and any other relevant applicable rules. The guidance contained in this Handbook should always be applied without prejudice to these rules and obligations. This guidance is based on recognized best practices and standards and it is recommended that International Organizations take this into consideration when designing or interpreting their data protection rules and policies for Humanitarian Action.

International Organizations enjoy privileges and immunities to ensure 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. They can therefore process Personal Data according to their own rules, subject to the internal monitoring and enforcement of their own compliance systems; in this regard they constitute their own “jurisdiction”. This aspect of International Organizations has specific implications, in particular for International Data Sharing, which will be discussed in detail in [Chapter 4: International Data Sharing](#).

2.5 DATA PROCESSING PRINCIPLES

Personal Data Processing undertaken by Humanitarian Organizations should comply with the following principles.

2.5.1 THE PRINCIPLE OF THE FAIRNESS AND LAWFULNESS OF PROCESSING

Personal Data should be processed fairly and lawfully. The lawfulness of the Processing requires a legal basis for Processing operations to take place, as detailed in [Chapter 3: Legal bases for Personal Data Processing](#). The other crucial component of Fairness of the Processing is transparency.

Any Processing of Personal Data should be transparent for the Data Subjects involved. The principle of transparency requires that at least a minimum amount of information concerning the Processing be provided to the Data Subjects at the moment of collection, albeit subject to the prevailing security and logistical conditions, as well as with regard to the possible urgent nature of the Processing. Any information and communication relating to the Processing of Personal Data should be easily accessible and easy to understand, which implies providing translations where necessary, and clear and plain language should be used. More detailed information about information notices that should be provided prior or at the time of data collection are described in greater detail in [Section 2.10.2: Information notices](#).

2.5.2 THE PURPOSE LIMITATION PRINCIPLE

At the time of collecting data, the Humanitarian Organization should determine and set out the specific purpose/s for which data are processed. The specific purposes should be explicit and legitimate. In particular, the specific purpose/s that may be of relevance in a humanitarian context may include, for example:

- providing humanitarian assistance and/or services to affected populations to sustain livelihoods
- restoring family links between people separated due to Humanitarian Emergencies
- providing protection to affected people and building respect for international human rights law/international humanitarian law (IHL), including documentation of individual violations
- providing medical assistance
- ensuring inclusion in national systems (for example for refugees)
- providing documentation or legal status/identity to, for example, displaced or stateless people
- protecting water and habitat.

Humanitarian Organizations should take care to consider and identify, as far as is possible in emergency circumstances, all possible purposes contemplated and that may be contemplated in any Further Processing prior to the collection of the data, so as to be as transparent as possible.

2.5.3 THE PRINCIPLE OF PROPORTIONALITY

The principle of proportionality is at the core of data protection law. It is applicable throughout the data Processing cycle and may be invoked at different stages of data Processing operations. It requires consideration of whether a particular action or measure related to the Processing of Personal Data is appropriate to its pursued aim (e.g. is the selected legitimate basis proportionate to the aim pursued? Are technical and organizational measures proportionate to the risks associated with the Processing?).

The data handled by Humanitarian Organizations should be adequate, relevant and not excessive for the purposes for which they are collected and processed. This requires, in particular, ensuring that only the Personal Data that are necessary to achieve the purposes (fixed in advance) are collected and further processed and that the period for which the data are stored, before being anonymized or deleted, is limited to the minimum necessary.³⁹

³⁹ See [Section 2.7: Data retention](#).

The principle of proportionality is particularly important for cross-functional needs assessments conducted by Humanitarian Organizations either internally or between agencies. When carrying out these assessments Humanitarian Organizations are at risk of gathering amounts of data that are excessive to the purpose, for example by conducting surveys with several hundred data fields to be filled, which may or may not be used at a later stage. In these situations, it is important to be able to distinguish between what is “nice to know” and what is “necessary to know” in order to assist beneficiaries. Humanitarian Organizations also need to weigh their need for data against the potential harm to individuals of such data being collected, as well as the risk of “assessment fatigue” and potentially raising unrealistic expectations among the people they seek to help.

Limiting the amount of data collected may not always be possible. For example, when a new Humanitarian Emergency arises, the full extent of humanitarian needs may not be known at the time of data collection. Therefore, the application of this principle may be restricted in exceptional circumstances and for a limited time if necessary for the protection of the Data Subject or of the rights and freedoms of others.

It is also possible that the purpose at the time of collection is particularly broad because of the emergency. In such cases, a large collection of data could be considered necessary. It could then be reduced later depending on circumstances. In considering whether a flexible interpretation of proportionality is acceptable when a new Humanitarian Emergency arises, the following factors should be taken into account:

- the urgency of the action
- proportionality between the amount of Personal Data collected and the goals of the Humanitarian Action
- the likely difficulties (due to logistical or security constraints) in reverting to the Data Subject to gather additional data, should additional specified purposes become foreseeable
- the objectives of the particular Humanitarian Organization’s action
- the nature and scope of the Personal Data that may be needed to fulfil the specified purposes
- the expectations of Data Subjects
- the sensitivity of the Personal Data concerned.

EXAMPLE:

A Humanitarian Organization collects Personal Data to provide humanitarian assistance to a group of vulnerable individuals in a disaster area. At the outset of the action, it was not possible to determine the specific needs of the people affected and what assistance and programmes would be required immediately or further down the line (e.g. the destruction of sanitation facilities could generate the risks of diseases spreading). Accordingly, the Humanitarian Organization in question engages in a broad data collection exercise with the purpose of fully assessing the needs of the people affected and designing response programmes. After the emergency has ended, it turned out that although Humanitarian Action was required, sanitation was restored in time to avoid the spread of diseases. As a result, the Humanitarian Organization may now need to delete the data initially acquired to address this specific concern.

In all cases, the necessity of retaining the data collected should be periodically reviewed to ensure application of the data minimization principle.

2.5.4 THE PRINCIPLE OF DATA MINIMIZATION

The principle of data minimization closely relates to the principle of proportionality. Data minimization seeks to ensure that only the minimum amount of Personal Data are processed to achieve the objective and purposes for which the data were collected. Data minimization requires limiting Personal Data Processing to the minimum amount and extent necessary. Personal Data should be deleted when they are no longer necessary for the purposes of the initial collection or for compatible Further Processing. Data must also be deleted when Data Subjects have withdrawn their Consent for Processing or justifiably object to the Processing. However, even in the above circumstances Personal Data may be retained if they are needed for legitimate historical, statistical, or scientific purposes, or if the Humanitarian Organization is under an applicable legal obligation to retain such data, taking into account the associated risks and implementing appropriate safeguards.

To determine whether the data are no longer necessary for the purposes for which they were collected, or for compatible Further Processing, Humanitarian Organizations should consider the following:

- Has the specified purpose been achieved?
- If not, are all data still necessary to achieve it? Is the specified purpose so unlikely to be achieved that retention no longer makes sense?
- Have inaccuracies affected the quality of Personal Data?
- Have any updates and significant changes rendered the original record of Personal Data unnecessary?
- Are the data necessary for legitimate historical, statistical, or scientific purposes? Is it proportionate to continue storing them, taking into account the

associated risks? Are appropriate data protection safeguards applied to this further storage?

- Have the Data Subject's circumstances changed, and do these new factors render the original record obsolete and irrelevant?

2.5.5 THE PRINCIPLE OF DATA QUALITY

Personal Data should be as accurate and up to date as possible. Every reasonable step should be taken to ensure that inaccurate Personal Data are deleted or corrected without undue delay, taking into account the purposes for which they are processed. The Humanitarian Organization should systematically review the information collected in order to confirm that it is reliable, accurate and up to date, in line with operational guidelines and procedures.

In considering the frequency of review, account should be taken of (i) logistical and security constraints, (ii) the purpose/s of Processing, and (iii) the potential consequences of data being inaccurate. All reasonable steps should be taken to minimize the possibility of making a decision that could be detrimental to an individual, such as excluding an individual from a humanitarian programme based on potentially incorrect data.

2.6 SPECIAL DATA PROCESSING SITUATIONS

The following are a few common data Processing situations that require more specific explanation.

2.6.1 HEALTH PURPOSES

Improper handling (including disclosure) of Health Data could cause significant harm to the individuals concerned. Accordingly, Health Data should be considered as particularly sensitive and specific guarantees should be implemented when Processing such data. This also applies to Sensitive Data. Health Data are also increasingly becoming a target for cyber-attacks. Humanitarian healthcare providers should process data in accordance with the WMA International Code of Medical Ethics⁴⁰ which includes specific professional obligations of confidentiality.

Humanitarian Organizations may process Health Data for purposes such as the following:

- preventive or occupational medicine, medical diagnosis, provision of care or treatment
- management of health-care services

⁴⁰ World Medical Association, *WMA International Code of Medical Ethics*:
<https://www.wma.net/policies-post/wma-international-code-of-medical-ethics/>.

- reasons of vital interest, including providing essential and life-saving medical assistance to the Data Subject
- public health, such as protecting against serious threats to health or ensuring high standards of quality and safety, *inter alia* for medicinal products or medical devices
- historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, subject to conditions and safeguards.

Health Data should be kept separate from other Personal Data, and should only be accessible by healthcare providers or personnel specifically delegated by the humanitarian healthcare providers to manage Health Data under confidentiality guarantees ensured by employment, consultant or other contracts and only for such predefined data management purposes, or by personnel carrying out research under confidentiality and other data protection guarantees ensured by employment, consultant or other contracts and only for such predefined research purposes.

Humanitarian Organizations engaged in protection or assistance activities may also process Health Data, for example, when this is necessary to locate persons unaccounted for (where Health Data may be required to identify and trace them) or to advocate for adequate treatment of individuals deprived of their liberty, or for the establishment of livelihood programmes addressing the needs of particularly vulnerable categories of beneficiaries (such as people suffering from malnutrition or particular diseases).⁴¹



Jonglei State, South Sudan. A war-wounded patient evacuated by a medical team.

⁴¹ See [Section 2.6.3: Further Processing](#).

2.6.2 ADMINISTRATIVE ACTIVITIES

Humanitarian Organizations typically process Personal Data for employment purposes, career management, assessments, direct marketing and other administrative requirements. In some instances this may also include sensitive Processing activities such as, for example, GPS tracking of its vehicles for fleet and security management. In some operational circumstances, the processing of staff Personal Data may be particularly sensitive due, for example, to the geopolitical conditions in which certain humanitarian assistance is provided. In these cases, additional safeguards will be necessary, to the extent possible, in the processing of such data.

2.6.3 FURTHER PROCESSING

Humanitarian Organizations may process Personal Data for purposes other than those initially specified at the time of collection where the Further Processing is compatible with the initial purposes, including where the Processing is necessary for historical, statistical or scientific purposes.

In order to ascertain whether a purpose of Further Processing is compatible with the purpose for which the data were initially collected, account should be taken of:

- the link between the initial purpose/s and the purpose/s of the intended Further Processing
- the situation in which the data were collected, including the reasonable expectations of the Data Subject as to their further use
- the nature of the Personal Data
- the consequences of the intended Further Processing for Data Subjects
- appropriate safeguards
- the extent to which such safeguards would protect the confidentiality of Personal Data and the anonymity of the Data Subject.

The situation in which the data were collected, including the reasonable expectations of the Data Subject as to its further use, is a particularly important factor, recognizing that when Data Subjects provide data for one purpose they generally understand that a range of associated humanitarian activities may also be involved and, in fact, may have an expectation that all possible humanitarian protection and assistance may be extended. This is particularly important in humanitarian situations, because an improperly narrow understanding of compatibility could prevent the delivery of humanitarian benefits to Data Subjects.

Consequently, purposes strictly linked to Humanitarian Action, and which do not incur any additional risks unforeseen in the consideration of the initial purpose, are likely to be compatible with each other and, if this is confirmed, Personal Data can legitimately be processed by Humanitarian Organizations beyond the specific purposes for which the Personal Data were originally collected, as long as the

Humanitarian Organization does so within the framework of Humanitarian Action. In principle, Further Processing should be permissible if this is necessary and proportionate to safeguard public security and the lives, integrity, health, dignity or security of affected individuals in Humanitarian Action. This requires a case-by-case assessment and cannot be presumed across the board.

Even where the purpose of Further Processing is exclusively related to Humanitarian Action, Processing for a new purpose may not be deemed compatible if the risks for the Data Subject outweigh the benefits of Further Processing, or if the Further Processing entails new risks. This analysis depends on the circumstances of the case. Circumstances leading to this conclusion include risks that Processing may be against the interests of the person to whom the information relates or his/her family, in particular, when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty, or their reputation. This can include consequences such as:

- harassment or persecution by authorities or Third Parties
- judicial prosecution
- social problems
- serious psychological suffering.

Examples of circumstances in which Further Processing may be considered incompatible include cases where the Personal Data have been collected as part of the information necessary to assist in the tracing of a Sought Person. Processing this information further in order to request that the relevant authorities carry out an investigation into the possible violations of the applicable law (for example, in the context of civilian population protection activities) may not be compatible as Further Processing. This is due to the possible detrimental consequences of the intended Further Processing for Data Subjects and the likely difficulty of providing appropriate safeguards.

Should the intended purpose of Further Processing not be compatible with the purpose for which the data were initially collected, the data should not be further processed, unless it is deemed appropriate to do so under another legal basis. In this case, additional measures may be required depending the basis that applies.⁴²

Further Processing of Personal Data should also not be considered compatible if the Processing conflicts with any legal, professional or other binding obligations of secrecy and confidentiality, or with the principle of “do no harm”.

Data aggregation and Anonymization may be used as a method of decreasing the sensitivity of the data to allow data use for ancillary cases.

⁴² See [Chapter 3: Legal bases for Personal Data Processing](#).

EXAMPLE:

Data collected to provide food and shelter during a humanitarian operation may also be used to plan the provision of medical services to displaced persons. However, Processing the data collected (if not aggregated/anonymized) to help plan the Humanitarian Organization's budgetary needs for the coming year cannot be deemed to be compatible Further Processing.

2.7 DATA RETENTION

Each category of data should be retained for a defined period (e.g. three months, a year, etc.). When it is not possible to determine at the time of collection how long data should be kept, an initial retention period should be set. Following the initial retention period, an assessment should be made as to whether the data should be deleted, or whether the data are still necessary to fulfil the purpose for which they were initially collected (or for a further legitimate purpose). If so, the initial retention period should be renewed for a limited period of time.

When data have been deleted, all copies of the data should also be deleted. If the data have been shared with Third Parties, the Humanitarian Organization should take reasonable steps to ensure such Third Parties also delete the data. This consideration should be taken into account in initial reflections as to whether to share data with Third Parties and should be expressed in any data sharing agreement.⁴³

2.8 DATA SECURITY AND PROCESSING SECURITY

2.8.1 INTRODUCTION

Data security is a crucial component of an effective data protection system. Personal Data should be processed in a manner that ensures appropriate security of the Personal Data, such as preventing unauthorized access to or use of Personal Data and the equipment used for the Processing. This is even more the case for the volatile environments in which Humanitarian Organizations often operate.

Any person acting under the authority of the Data Controller who has access to Personal Data should not process them except in a manner compliant with any applicable policies as explained in the present Handbook.

⁴³ See [Section 2.12: Data sharing and International Data Sharing](#) and [Chapter 4: International Data Sharing](#).

In order to maintain security, the Data Controller should assess the specific risks inherent in the Processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security (taking into account available technology, prevailing security and logistical conditions and the costs of implementation) in relation to the nature of the Personal Data to be protected and the related risks. This includes measures involving:

- training of staff and partners
- management of access rights to databases containing Personal Data
- physical security of databases (access regulation, water and temperature damage, etc.)
- IT security (including password protection, safe transfer of data, encryption, regular backups, etc.)
- discretion clauses
- data sharing agreements with partners and Third Parties
- methods of destruction of Personal Data
- standard operating procedures for data management and retention
- any other appropriate measures.

These measures are intended to ensure that Personal Data are kept secure, both technically and organizationally, and are protected by reasonable and appropriate measures against misuse, unauthorized modification, copying, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer (collectively, “Data Breach”). Data security measures should vary depending, *inter alia*, on the:

- type of operation
- level of assessed data protection risks
- nature and sensitivity of the Personal Data involved
- form or format of storage, transfer and sharing of data
- environment/location of the specific Personal Data
- prevailing security and logistical conditions.

Data security measures should be routinely reviewed and upgraded to ensure a level of data protection that is appropriate to the degree of sensitivity applied to Personal Data, as well as the possible development of new technologies enabling enhanced security.

The Data Controller is responsible for:

- setting up an information security management system. This includes establishing and regularly updating a data security policy based on internationally accepted standards and on a risk assessment. The policy should consist of, for example, physical security guidelines, IT security policy, email security guidelines, IT equipment usage guidelines, guidelines for information classification (i.e. classifying information as public, internal, confidential and strictly confidential), a contingency plan, and document destruction guidelines.

- developing the communication infrastructure and databases in order to preserve the confidentiality, integrity and availability of data, in compliance with the security policy.
- taking all appropriate measures to protect the security of data processed in the Data Controller's information system.
- granting and administering access to databases containing Personal Data, including ensuring access is granted on a need-to-know basis.
- the security of the facilities which enable authorized personnel to access the system.
- ensuring that the personnel given access to data are in a position to fully respect security rules. This includes relevant training, a pledge of discretion and/or duty of confidentiality clause in the employment contract to be signed before access to databases is granted.
- maintaining a register of personnel having access to each database, and updating it when appropriate (e.g. personnel being given different responsibilities who no longer require access).
- if feasible, keeping a historical log and potentially running audits of personnel having had access to a database, for as long as the data processed by such personnel are present in the database.

Personnel should process data within the limits of the Processing rights granted to them. Personnel with higher access rights or responsible for administering access rights may be subject to additional contractual obligations of confidentiality and non-disclosure.

2.8.2 PHYSICAL SECURITY

Each Data Controller is responsible for:

- laying down security rules defining procedural, technical and administrative security controls that ensure appropriate levels of confidentiality, and physical integrity and availability of databases (whether physical or IT based), based on the prevailing risks identified
- ensuring that personnel are informed of such security rules and comply with them
- developing appropriate control mechanisms to ensure that the security of data is maintained
- ensuring adequate electrical and fire safety standards are applied to storage locations
- ensuring storage volumes are kept to a strict necessary minimum.

2.8.3 IT SECURITY

The Data Controller should:

- lay down security rules defining procedural, technical and administrative controls that ensure appropriate levels of confidentiality, integrity and availability for the information systems used, based on risk assessment
- develop appropriate control mechanisms to ensure that data security is maintained
- introduce specific security rules for a part of the IT communication infrastructure, a database or a specific department if necessary, for instance where particularly sensitive or critical Personal Data are being processed.

All email correspondence, internal and external, containing Personal Data should be processed on a need-to-know basis. Recipients of email correspondence should be carefully selected to avoid unnecessary dissemination of Personal Data to individuals who do not need such Data in the context of their role. Private email accounts should not be used to transfer Personal Data.

Remote access to servers and the use of home-based computers should comply with the standards set out in the Data Controller's IT Security Policy. Unless absolutely necessary for operational reasons, the use of internet outlets and unsecured wireless connections to retrieve, exchange, transmit or transfer Personal Data should be avoided.

Staff members handling Personal Data should take due care when connecting remotely to the Data Controller's servers. Passwords should always be protected, regularly changed and not be automatically entered through 'keychain' functions.⁴⁴ Staff should check that they have logged off properly from computer systems and that open browsers have been closed.

Special consideration must be given to securing laptops, smartphones and other portable media equipment, especially when working in a difficult environment. Portable media equipment should be stored in safe and secure locations at all times.

Portable or removable devices should not be used to store documents containing Personal Data classified as sensitive. If this is unavoidable, Personal Data should be transferred to appropriate computer systems and database applications as soon as possible. If flash memory such as USB flash drives and memory cards are used to temporarily store Personal Data, they should be kept safe and the electronic record must be encrypted. Information should be deleted from the portable or removable device once it has been stored properly, if no longer needed on the portable device.

⁴⁴ A keychain or password manager is an application or hardware function that enables users to store and organize several passwords centrally under one master password.

Effective recovery mechanisms and backup procedures should cover all electronic records, and the relevant information and communications technology (ICT) officer should ensure that backup procedures are performed on a regular basis. The frequency of backup procedures should vary according to the sensitivity of the Personal Data and available technical resources. Electronic records should be automated to allow for easy recovery in situations where backup procedures are difficult due to, *inter alia*, regular power outage, system failure or disasters.

When electronic records and database applications are no longer needed, the Data Controller should coordinate with the relevant ICT officer to ensure their permanent deletion.

2.8.4 DUTY OF DISCRETION AND STAFF CONDUCT

The duty of discretion is a key element of Personal Data security. The duty of discretion involves:

- all personnel and external consultants signing discretion and confidentiality agreements or clauses as part of their employment/consulting contract. This requirement goes together with the requirement that personnel should only process data in accordance with the Data Controller's instructions.
- any external Data Processor being contractually bound by confidentiality clauses. This requirement goes together with the requirement that the Data Processor should only process data in accordance with the Data Controller's instructions.
- the strict application of the guidelines for information classification based on their confidentiality status.
- ensuring that Data Subject requests are properly addressed and accurately recorded in the Data Subject's file in a secure and confidential manner, and that such requests are not shared with Third Parties.
- limiting the risk of leaks by having only authorized personnel in charge of the collection and management of data from confidential sources, and ensuring these personnel access documents according to the applicable guidelines for information classification.

Personnel are responsible for attributing levels of confidentiality to the data they process based on the applicable guidelines for information classification, and for observing the confidentiality of the data they consult, transmit or use for external Processing purposes. Personnel who originally attributed the level of confidentiality may, at any time, modify the level of confidentiality that they have attributed to data, as appropriate.

2.8.5 CONTINGENCY PLANNING

The Data Controller is responsible for devising and implementing a plan for protecting, evacuating or safely destroying records in case of emergency.

2.8.6 DESTRUCTION METHODS

When it is established that retention of Personal Data is no longer necessary, all records and backups should be safely destroyed or rendered anonymous. The method of destruction shall depend, *inter alia*, on the following factors:

- the nature and sensitivity of the Personal Data
- the format and storage medium
- the volume of electronic and paper records.

The Controller should conduct a sensitivity assessment prior to destruction to ensure that appropriate methods of destruction are used to eliminate Personal Data. In this regard, the following three paragraphs are based on information taken from the IOM Data Protection Manual:⁴⁵

Paper records should be destroyed by using methods such as shredding or burning, in a way that does not allow for future use or reconstruction. If it is decided that paper records should be converted into digital records, following accurate conversion of paper records to electronic format, all traces of paper records should be destroyed, unless retention of paper records is required by applicable national law, or unless a paper copy should be kept for archiving purposes. The destruction of large volumes of paper records may be outsourced to specialized companies. In these circumstances the Data Controller should ensure that, throughout the chain of custody, the confidentiality of Personal Data, the submission of disposal records and the certification of destruction form part of the contractual obligations of the Data Processors, and that the Data Processors comply with these obligations.

The destruction of electronic records should be referred to the relevant ICT personnel because the erasure features on computer systems do not necessarily ensure complete elimination. Upon instruction, the relevant ICT personnel should ensure that all traces of Personal Data are completely removed from computer systems and other software. Disk drives and database applications should be purged and all rewritable media such as, *inter alia*, CDs, DVDs, microfiches, videotapes and audio tapes that are used to store Personal Data should be erased before reuse. Physical measures of destroying electronic records such as recycling, pulverizing or burning should be strictly monitored.

⁴⁵ International Organization for Migration (IOM), *Data Protection Manual*, 2010, pp. 83–84: <https://publications.iom.int/books/iom-data-protection-manual>.

The Data Controller should ensure that all relevant contracts of service, MOUs, agreements and written transfer or Processing contracts include a retention period for the destruction of Personal Data after the fulfilment of the specified purpose. Third parties should return Personal Data to the Data Controller and certify that all copies of the Personal Data have been destroyed, including the Personal Data disclosed to its authorized agents and sub-contractors. Disposal records indicating time and method of destruction, as well as the nature of the records destroyed, should be maintained and attached to project or evaluation reports.

2.8.7 OTHER MEASURES

Data security also requires appropriate internal organizational measures, including regular internal dissemination of data security rules and their obligations under data protection law or internal rules for organizations enjoying privileges and immunities to all employees, especially regarding their obligations of confidentiality.

Each Data Controller should attribute the role of data security officer to one or more persons of their staff (possibly Admin/IT) to carry out security operations. The security officer should, in particular:

- ensure compliance with the applicable security procedures and rules
- update these procedures, as and when required
- conduct further training on data security for personnel.

2.9 THE PRINCIPLE OF ACCOUNTABILITY

The principle of accountability is premised on the responsibility of Data Controllers to comply with the above principles and the requirement that they be in a position to demonstrate that adequate and proportionate measures have been undertaken within their respective organizations to ensure compliance with them.

This can include measures such as the following, which are all strongly recommended in order to allow Humanitarian Organizations to meet data protection requirements:

- drafting Personal Data Processing policies (including Processing Security policies)
- keeping internal records of data Processing activities
- creating an independent body to oversee the implementation of the applicable data protection rules, such as a Data Protection Office, and appointing a Data Protection Officer (DPO)
- implementing data protection training programmes for all staff
- performing Data Protection Impact Assessments (DPIAs)⁴⁶
- registering with the competent authorities (including data protection authorities), if legally required and not incompatible with the principle of “do no harm”.

⁴⁶ See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

2.10 INFORMATION

In line with the principle of transparency, some information regarding the Processing of Personal Data should be provided to Data Subjects. As a rule, this information should be provided before Personal Data are processed, although this principle may be limited when it is necessary to provide emergency aid to individuals.

Data Subjects should receive information orally and/or in writing. This should be done as transparently as circumstances allow and, if possible, directly to the individuals concerned. If this is not possible, the Humanitarian Organization should consider providing information by other means, for example, making it available online, or on flyers or posters displayed in a place and form that can easily be accessed (public spaces, markets, places of worship and/or the organizations' offices), radio communication, or discussion with representatives of the community. Data Subjects should be kept informed, in so far as practicable, of the Processing of their Personal Data in relation to the action taken on their behalf, and of the ensuing results.

The information given may vary, depending on whether the data are collected directly from the Data Subject or not.

2.10.1 DATA COLLECTED FROM THE DATA SUBJECT

Personal Data may be collected directly from the Data Subject under the following legal bases:⁴⁷

- vital interest of the Data Subject or of another person
- public interest
- individual Consent
- legitimate interest of the Humanitarian Organization
- legal or contractual obligation.

Some of the information to be provided to Data Subjects in each of the above cases will vary depending on the particular circumstances. A priority in this respect is that the information provided must be sufficient to enable them to exercise their data protection rights effectively.⁴⁸

⁴⁷ See [Chapter 3: Legal bases for Personal Data Processing](#).

⁴⁸ See [Section 2.11: Rights of Data Subjects](#).

2.10.2 INFORMATION NOTICES

In the specific cases where Consent may be used as the legal basis,⁴⁹ the individual must be put in a position to fully appreciate the risks and benefits of data Processing, otherwise Consent may not be considered valid.

When using Consent or when the Data Subjects are exercising their rights to object to the Processing or to access, rectify and erase the data, detailed information will need to be provided. It is important to note that the Data Subject may object to the Processing or withdraw his/her Consent at any time. The following are the types of information to be provided when Consent is the legal basis:

- the identity and contact details of the Data Controller
- the specific purpose for Processing of his/her Personal Data and an explanation of the potential risks and benefits
- the fact that the Data Controller may process his/her Personal Data for purposes other than those initially specified at the time of collection, if compatible with a specific purpose mentioned above and an indication of these further compatible purposes
- the fact that if he/she has given Consent, he/she can withdraw it at any time
- circumstances in which it might not be possible to treat his/her Personal Data confidentially
- the Data Subject's rights to object to the Processing and to access, correct and delete their Personal Data; how to exercise such rights and the possible limitations on the exercise of his/her rights
- to which third countries or International Organization/s the Data Controller may need to transfer the data in order to achieve the purpose of the initial collection and Further Processing
- the period for which the Personal Data will be kept or at least the criteria to determine it and any steps taken to ensure that records are accurate and kept up to date
- with which other organizations, such as authorities in the country of data collection the Personal Data may be shared
- in case decisions are taken on the basis of automated Processing, information about the logic involved
- an indication of the security measures implemented by the Data Controller regarding the data Processing.

Under other legal bases for Processing, the responsibility for conducting a risk analysis rests with the Data Controller, and it is sufficient to provide more basic information. The following is recommended as the minimum information that should be provided in the case of a legal basis other than Consent:

- the identity and contact details of the Data Controller
- the specific purpose for Processing of his/her Personal Data

⁴⁹ See [Section 3.2: Consent](#).

- whom to contact in case of any questions concerning the Processing of their Personal Data
- with whom the data will be shared, in particular if it may be shared with authorities (e.g. law enforcement authorities) or entities in another territory or jurisdiction.

Additional information must be provided where necessary to enable individuals to Consent and exercise their rights of access, objection, rectification, erasure and/or if the Data Subject requests more information.⁵⁰

In exceptional circumstances where, due to prevailing security and logistical constraints, including difficulties gaining access to the field, it is not possible to provide this information immediately or at the place where individuals are located, or where the data have not been collected directly from the Data Subject, the information should be made available as soon as possible in a way that is easy for individuals to access and understand.⁵¹ Humanitarian Organizations should also refrain from collecting extensive data sets from beneficiaries until this information can be adequately provided, unless absolutely necessary for humanitarian purposes.

2.10.3 DATA NOT COLLECTED FROM THE DATA SUBJECT

Where the Personal Data have not been obtained from the Data Subject, the information set out under Section 2.10.2 above, depending on the legal basis used for the collection of data, should be provided to the Data Subject within a reasonable period after obtaining this data, having regard to the specific circumstances in which the data are processed or, if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed, subject to logistical and security constraints. This requirement will not apply where the Data Subject already has the information or where providing it is impossible or would involve a disproportionate effort, in which case the measures outlined above in 2.10 Information should be considered.

EXAMPLE:

Information may be provided after obtaining the data, for example, where a protection case is documented involving multiple victims and the information is collected from only one of them or from a third source, or where lists of displaced persons are collected from authorities or from other organizations for the distribution of aid.

⁵⁰ See [Section 2.10: Information](#) and [Section 3.2: Consent](#).

⁵¹ See [Section 2.10: Information](#).

2.11 RIGHTS OF DATA SUBJECTS

2.11.1 INTRODUCTION

The respect of Data Subjects' rights is a key element of data protection. However, the exercise of these rights is subject to conditions and may be limited as explained below.

An individual should be able to exercise these rights using the internal procedures of the relevant Humanitarian Organization, such as by lodging an inquiry or complaint with the organization's DPO. However, depending on the applicable law, and in cases where the Data Controller is not an International Organization with immunity from jurisdiction, the individual may also have the right to bring a claim in court or with a data protection authority. In the case of International Organizations, claims may be brought before an equivalent body responsible for independent review of cases for the organization.⁵²

2.11.2 ACCESS

A Data Subject should be able to make an access request orally or in writing to the Humanitarian Organization. Data Subjects should be given an opportunity to review and verify their Personal Data. The exercise of this right may be restricted if necessary for the protection of the rights and freedoms of others, or if necessary for the documentation of alleged violations of international humanitarian law or human rights law.

With due consideration for the prevailing situation and its security constraints, Data Subjects should be given the opportunity to obtain confirmation from the Humanitarian Organization, at reasonable intervals and free of charge, whether their Personal Data are being processed or not. Where such Personal Data are being processed, Data Subjects should be able to obtain access to them, except as otherwise provided below.

The Humanitarian Organization's staff should not reveal any information relating to Data Subjects, unless they are provided with satisfactory proof of identity from the Data Subjects and/or their authorized representative.

Access to documents does not apply when overriding interests require that access not be given. Thus, compliance by Humanitarian Organizations with a Data Subject's access request may be restricted as a result of the overriding public interests or interests of others. This is particularly the case where access cannot be provided

⁵² See INTERPOL Commission for the Control of Files: <https://www.interpol.int/About-INTERPOL/Commission-for-the-Control-of-Files-CCF> and ICRC Data Protection Commission: <https://www.icrc.org/en/document/icrc-data-protection-independent-control-commission>.

without revealing the Personal Data of others, except where the document or information can be meaningfully redacted to blank out any reference to such other Data Subject/s without disproportionate effort, or where the consent of such other Data Subject/s to the disclosure has been obtained, again without disproportionate effort.

Access that would jeopardize the ability of a Humanitarian Organization to pursue the objectives of its Humanitarian Action or that creates risks for the security of its staff will always constitute an overriding interest. This may also be the case for internal documents of the Humanitarian Organizations, disclosure of which may have an adverse effect on Humanitarian Action. In such cases, the Humanitarian Organization should make every effort to document the nature of the overriding interests, to the extent possible and subject to prevailing circumstances.

Communication to Data Subjects on the information set out in this section should be given in an intelligible form, which means that the Humanitarian Organization may have to explain the Processing to the Data Subjects in more detail or provide translations. For example, just quoting technical abbreviations or medical terms in response to an access request will usually not suffice, even if only such abbreviations or terms are stored.



O. Saltbones/ICRC

Pristina, Kosovo.* Fresh flowers attached to photographs of people who have been missing since the war ended in 1999.

* UN Security Council Resolution 1244.

It may be appropriate to disclose Personal Data to family members or legal guardians in the case of missing, unconscious or deceased Data Subjects or of Data Subjects' families seeking access for humanitarian or administrative reasons or for family history research. Here too, the staff of Humanitarian Organizations should not reveal any information unless they are provided with satisfactory proof of identity of the requesting person and proof of legal guardianship/family link, as appropriate, and they have made a reasonable effort to establish the validity of the request.

2.11.3 CORRECTION

The Data Subject should also be able to ensure that the Humanitarian Organization corrects any inaccurate Personal Data relating to him/her. Having regard to the purposes for which data were processed, the Data Subject should be able to correct incomplete Personal Data, for instance by providing supplementary information.

When this involves simply correcting factual data (e.g. requesting the correction of the spelling of a name, change of address or telephone number), proof of inaccuracy may not be crucial. If, however, such requests are linked to a Humanitarian Organization's findings or records (such as the Data Subject's legal identity, or the correct place of residence for the delivery of legal documents, or more sensitive information about the humanitarian status of, or medical information concerning, the Data Subject), the Data Controller may need to demand proof of the alleged inaccuracy and assess the credibility of the assertion. Such demands should not place an unreasonable burden of proof on the Data Subject and thereby preclude Data Subjects from having their data corrected. In addition, Humanitarian Organization staff should require satisfactory proof of identity from the Data Subjects and/or their authorized representative before carrying out any correction.

2.11.4 RIGHT TO ERASURE

A Data Subject should be able to have his/her own Personal Data erased from the Humanitarian Organization's databases where:

- the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed and/or further processed
- the Data Subject has withdrawn his/her Consent for Processing, and there is no other basis for the Processing of the data⁵³
- the Data Subject successfully objects to the Processing of Personal Data concerning him/her⁵⁴
- the Processing does not comply with the applicable data protection and privacy laws, regulations and policies.

⁵³ See [Section 3.2: Consent](#).

⁵⁴ See [Section 3.4: Important grounds of public interest](#) and [Section 3.5: Legitimate interest](#).

The exercise of this right may be restricted if necessary for the protection of the Data Subject or the rights and freedoms of others, for the documentation of alleged violations of international humanitarian law or human rights law, for reasons of public interest in the area of public health, for compliance with an applicable legal obligation, for the establishment, exercise or defence of legal claims, or for legitimate historical or research purposes, subject to appropriate safeguards and taking into account the risks for and the interests of the Data Subject. This can include the interest in maintaining archives that represent the common heritage of humanity. In addition, Humanitarian Organization staff should require proof of identify that satisfies them that the Data Subjects are who they say they are before carrying out any erasure.

EXAMPLE:

A Humanitarian Organization suspects that a request for erasure is being made under pressure from a Third Party, and that erasure would prevent the protection of the Data Subject or documentation of an alleged violation of international humanitarian law or human rights law. In such a case, the Humanitarian Organization would be justified in refusing to erase the data.

2.11.5 RIGHT TO OBJECT

Data Subjects have the right to object, on compelling legitimate grounds relating to their particular situation, at any time, to the Processing of Personal Data concerning them.

The exercise of this right may be restricted if necessary if the Humanitarian Organization has compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject. Such grounds may include, for example, the protection of the Data Subject or the rights and freedoms of others, the documentation of alleged violations of international humanitarian law or human rights law, the establishment, exercise or defence of legal claims, or legitimate historical or research purposes, subject to appropriate safeguards and taking into account the risks for and the interests of the Data Subject. In these cases, the Humanitarian Organization should:

- inform the organization's DPO, if there is one
- inform, if possible, the Data Subject of the Humanitarian Organization's intention to continue to process data on this basis
- inform, if possible, the Data Subject of his/her right to seek a review of the Humanitarian Organization's decision by the DPO or the competent state authority, court or equivalent body in the case of International Organizations.

In addition, Humanitarian Organization staff should require proof of identify that satisfies them that the Data Subjects are who they say they are before accepting an objection.

2.12 DATA SHARING AND INTERNATIONAL DATA SHARING

Humanitarian Emergencies routinely require Humanitarian Organizations to share Personal Data with Data Processors and Third Parties, including those based in other countries, or with International Organizations. Data protection laws restrict the sharing of and access to Personal Data with Third Parties, in particular in case of transfers across borders or jurisdictions. Also, many data protection laws restrict International Data Sharing, which means any act of making Personal Data accessible outside the country in which they were originally collected or processed, as well as to a different entity within the same Humanitarian Organization not enjoying the status of International Organization, or to a Third Party, via electronic means, the internet, or others.⁵⁵

Data sharing requires due regard to all the various conditions set out in this Handbook. For example, since data sharing is a form of Processing, there must be a legal basis for it and it can only take place for the specific purpose for which the data were initially collected or further processed. In addition, Data Subjects have rights in relation to data sharing and must be given information about it. The conditions governing International Data Sharing are given in [Chapter 4: International Data Sharing](#).

⁵⁵ See [Chapter 4: International Data Sharing](#).



CHAPTER 3

LEGAL BASES FOR PERSONAL DATA PROCESSING

3.1 INTRODUCTION

Under the principle of the lawfulness of data Processing outlined in [Chapter 2: Basic principles of data protection](#), a legitimate legal basis is required in order for Personal Data Processing operations to take place.

In their humanitarian work, Humanitarian Organizations may rely on the following legal bases to process Personal Data:

- vital interest of the Data Subject or of another person
- public interest
- Consent
- legitimate interest
- performance of a contract
- compliance with a legal obligation.

In the emergency situations in which Humanitarian Organizations usually operate it can be difficult to fulfil the basic conditions of valid Consent, in particular that it is informed and freely given. For example, this can be the case where consenting to the Processing of Personal Data is a precondition to receive assistance. It could also apply to human resources, for example, if consenting to the Processing is a condition for recruitment.

Processing by Humanitarian Organizations may often be based on vital interest or on important grounds of public interest,⁵⁶ for example in the performance of a mandate established under national or international law. This would require that the following conditions be met:

- in the case of vital interest, having sufficient elements to consider that in the absence of Processing the individual could be at risk of physical or moral harm. In the case of important grounds of public interest, being clear that the specific Processing operation is within a mandate established for the Humanitarian Organization under national, regional or international law, or that the Humanitarian Organization is otherwise performing a specific task or function that is in the public interest and is laid down by law.
- providing clear information to the individual as to the proposed Processing operation.
- ensuring the individual has a say and is in a position to exercise the right to object.⁵⁷ In any case, the opportunity to object to the Processing should be offered as soon and as clearly as possible, preferably at the moment of data collection. If the Data Subject provides adequate justification for his or her objection to the Processing, and if the Processing is not necessary for any other

⁵⁶ See [Section 3.3: Vital interest](#) and [Section 3.4: Important Grounds of Public interest](#).

⁵⁷ See [Chapter 2: Basic principles of data protection](#).

legal basis (e.g. [Section 3.3: Vital interest](#) or [Section 3.4: Important Grounds of Public interest](#)), then the Processing of the Data Subject's Personal Data should cease.

Relying on an appropriate legal basis does not discharge a Humanitarian Organization of its responsibility to assess the risk, for an individual, a given group, or the Humanitarian Organization itself of collecting, storing or using Personal Data. In cases involving particularly high risks, Humanitarian Organizations should consider whether it is not more appropriate to refrain from collecting and/or Processing the data in the first place. Such risks may be immediately evident from the Humanitarian Organization's experience or hidden in the complexity of the data flows inherent in a new technological solution. The performance of a Data Protection Impact Assessment (DPIA) therefore remains a key tool to ensure that all relevant risks are identified and mitigated.⁵⁸

3.2 CONSENT

Consent is the most popular and often the preferred legal basis for Personal Data Processing. However, given the vulnerability of most beneficiaries and the nature of Humanitarian Emergencies, many Humanitarian Organizations will not be in a position to rely on Consent for most of their Personal Data Processing. In particular, the choice of another legal basis is appropriate when:

- the Data Subject is not physically in a position to be informed and give free Consent, either because, for example, he/she is a Sought Person, or he/she is unconscious.
- the Humanitarian Organization is not in a position to inform and obtain the Consent of the Data Subject due to the prevailing security or logistical conditions in the area of operations.
- the Humanitarian Organization is not in a position to inform and obtain the Consent of the Data Subjects due to the scale of the operation that needs to be carried out. This can be the case, for example, (i) when preparing lists for distribution of humanitarian assistance to large numbers of displaced people, or (ii) when authorities provide Humanitarian Organizations with lists of protected persons, under a provision deriving from international humanitarian law or human rights law.
- in the organization's assessment, the Consent of the Data Subject cannot be valid due, for example, to the Data Subject being particularly vulnerable (e.g. children, elderly or disabled persons) at the time of giving Consent, or having no real choice to refuse Consent due to a situation of need and vulnerability, including a lack of alternative to the specific assistance being offered and the data Processing involved.

⁵⁸ See [Chapter 2: Basic principles of data protection](#).

- new technologies are involved, characterized by complex data flows and multiple stakeholders, including Data Processors and sub-Data Processors in multiple jurisdictions. This makes it difficult for an individual to fully appreciate the risks and benefits of a Processing operation and, therefore, take the responsibility for it as entailed by giving Consent. In this case, other legal bases, which require Humanitarian Organizations to take more responsibility for the assessment of risks and benefits of Processing, would be more appropriate.

It should be noted that obtaining Consent is not the same as providing information about data Processing ([Section 2.10: Information](#)). That is, even when Consent cannot be used, informational requirements still apply, including information on the rights to objection, erasure, access and rectification.

The following requirements must be fulfilled in order for Consent to be valid.

3.2.1 UNAMBIGUOUS

Consent should be fully informed and freely given by any appropriate method. This means that the Data Subject signifies their agreement to the Processing of their Personal Data. Consent may be given in writing or, where written consent is not possible, orally or by another clearly affirmative action by the Data Subject (or by his or her guardian, as applicable).

3.2.2 TIMING

Consent should be obtained at the time of collection or as soon as it is reasonably practical thereafter.

3.2.3 VALIDITY

Consent should not be regarded as freely given if the Data Subject has no genuine and free choice or is unable to refuse or withdraw Consent without detriment or has not been informed sufficiently in order to understand the consequences of the Personal Data Processing.

3.2.4 VULNERABILITY

The Data Subject's vulnerability should be taken into account when considering the validity of Consent. Assessing vulnerability involves understanding the social, cultural and religious norms of the group to which Data Subjects belongs and ensuring that each Data Subject is treated individually as the owner of his/her Personal Data. Respect for the individual implies that each person is regarded as autonomous, independent and free to make his/her own choices.

Vulnerability varies depending on the circumstances. In this respect, the following factors should be considered:⁵⁹

- the characteristics of the Data Subject, such as illiteracy, disability, age, health status, gender and sexual orientation
- the location of the Data Subject, such as a detention facility, resettlement camp, remote area
- environmental and other factors, such as unfamiliar surroundings, foreign language and concepts
- the Data Subject's position in relation to others, such as belonging to a minority group or ethnicity
- social, cultural and religious norms of families, communities, or other groups to which Data Subjects belong
- the complexity of the envisaged Processing operation, particularly if complex new technologies are employed.

EXAMPLE:

A Humanitarian Organization carries out an assessment of a Humanitarian Emergency. In doing so, it collects data on possible beneficiaries, including information about household livelihood and specific vulnerabilities with a view to developing a suitable assistance programme, which may include nutrition, health and protection components. This involves collecting and Processing a great deal of Personal Data. The organization should inform the individuals it interviews about the purposes for which the data collection will be used, but it would not be meaningful to base the data collection on their Consent. Such individuals have no meaningful possibility to give Consent to data collection, because they are in an extremely vulnerable position and have no genuine choice but to accept whatever Processing operation may be involved in accepting the aid offered. Another legal basis should be identified, and the relevant information provided, including the option to object to the envisaged Processing.

3.2.5 CHILDREN

Children are a particularly vulnerable category of Data Subjects, and the best interests of the child are paramount in all decisions affecting them. While the views and opinions of children should be respected at all times, particular care should be taken to establish whether the child fully understands the risks and benefits involved in a Processing operation and to exercise his/her right to object and to provide valid Consent where applicable. Assessment of the vulnerability of children will depend on the child's age and maturity.

⁵⁹ International Organization for Migration (IOM), Data Protection Manual (2010), pp. 45–48: <https://publications.iom.int/books/iom-data-protection-manual>.



P. Moore/CRC

A child receives a message from his family at the CAJED* transit and orientation centre for children formerly associated with armed forces or groups. North Kivu province, Democratic Republic of the Congo.

The Consent of the child's parent or legal guardian may be necessary if the child does not have the legal capacity to Consent. The following factors should be taken into account:

- providing full information to the parent or legal guardian and obtaining the signature of the parent or guardian to indicate their Consent
- ensuring the Data Subject is clearly informed and his/her views are taken into account.

3.2.6 INFORMED

Consent should be informed if it is to be accepted as the legal basis for Processing. This requires that the Data Subject receive explanations in simple, jargon-free language, which allows for full appreciation and understanding of the circumstances, risks, and benefits of Processing.⁶⁰

* CAJED (Concerted Action for Disadvantaged Young People and Children – Concert d'actions pour jeunes et enfants défavorisés).

⁶⁰ See [Section 2.10: Information](#).

3.2.7 DOCUMENTED

Where Processing is based on the Data Subject's Consent, it is important to keep a record of it to be able to demonstrate that the Data Subject has consented to the Processing. This may be done by requesting a signature or cross mark witnessed by a Humanitarian Organization or, in case of oral Consent, documentation by a Humanitarian Organization that Consent has been obtained. The practice, not unknown in the humanitarian world, to ask for the impression of a fingerprint solely to confirm Consent is highly problematic since it can amount to the collection of biometric data and should therefore be avoided. For an analysis of the risks involved in the collection of biometric data, see [Chapter 8: Biometrics](#).

When using Consent, it is important to record any limitations/conditions for its use, and the specific purpose for which Consent is obtained. These details should also be recorded in all databases used by Humanitarian Organizations to process the data in question and should accompany the data throughout the Processing.

Where Consent has not been recorded, or no record of Consent can be found, the data should not be processed further (including transferred to a Third Party if there is no record of Consent for the transfer) unless it is possible to do so under a legal basis other than Consent (e.g. vital interest, legitimate interest or public interest).

3.2.8 WITHHOLDING/WITHDRAWING CONSENT

If Data Subjects expressly withhold Consent, they should be advised about the implications, including the effect this may have on assistance that might or might not be rendered by Humanitarian Organizations and/or Third Party organizations. If, however, assistance could not be provided in the absence of Consent, note that Consent could not be considered as a legal basis for the Processing.⁶¹

Data Subjects have the right to object to the Processing and withdraw any Consent previously given at any stage of data Processing. In cases in which a Humanitarian Organization suspects that Consent is being withdrawn under pressure from Third Parties, it is likely that the Humanitarian Organization may be in a position to continue Processing the Personal Data of the Data Subject on another basis, such as vital interests being at stake (see 3.3 below).

⁶¹ See [Section 3.2: Consent](#), fourth bullet point.

3.3 VITAL INTEREST

When Consent cannot be validly obtained, Personal Data may still be processed if the Humanitarian Organization establishes that this is in the vital interest of the Data Subject or of another person, i.e. where data Processing is necessary in order to protect an interest which is essential for the Data Subject's life, integrity, health, dignity, or security or that of another person.

Considering the nature of Humanitarian Organizations' work, and the emergency situations in which they operate, Processing of data by Humanitarian Organizations may be based on the vital interest of a Data Subject or another person in the following cases:

- The Humanitarian Organization is dealing with cases of Sought Persons.
- The Humanitarian Organization is assisting authorities with the identification of human remains and/or tracing the family of the deceased. In this case the Personal Data would be processed in the vital interest of the family members.
- The Humanitarian Organization is assisting an individual who is unconscious or otherwise at risk, but unable to communicate Consent.
- The Humanitarian Organization is providing medical care or assistance.
- The Processing, including disclosure, of information is the most appropriate response to an imminent threat against the physical and mental integrity of the Data Subjects or other persons.
- The Processing is necessary to provide for the essential needs of an individual or a community during, or in the aftermath of, a Humanitarian Emergency.

In these cases, however, the Humanitarian Organization should, if possible, ensure that the Data Subjects are aware of the Processing as soon as possible, that they have sufficient knowledge to understand and appreciate the specified purpose(s) for which Personal Data are collected and processed, and are in a position to object to the Processing if they so wish. This can be achieved preferably through direct explanations at the moment of the collection and, for example, during distributions of assistance, using posters, group explanations or by making further information available on leaflets or on web sites when beneficiaries are registered or aid is distributed.⁶²

⁶² See [Section 2.5.1: The principle of the fairness and lawfulness of Processing](#) and [Section 2.10: Information](#).

EXAMPLE:

A Humanitarian Organization needs to collect Personal Data from vulnerable individuals following a natural disaster in order to provide vital assistance (e.g. food, water, medical assistance, etc.). It may use the vital interests of the individuals as the legal basis for the collection of Personal Data, without the need to obtain their Consent. However, it should 1) ensure that this legal basis is used only to provide such assistance; 2) offer the individuals the right to object; and 3) process the data collected in accordance with its privacy policy, which should be available to Data Subjects upon request. It should provide all relevant information about the data Processing, for example through posters, or group explanations, or by making further information available on leaflets or web sites when beneficiaries are registered or aid is distributed.

3.4 IMPORTANT GROUNDS OF PUBLIC INTEREST

Important grounds of public interest are triggered when the activity in question is part of a humanitarian mandate established under national or international law or is otherwise an activity in the public interest laid down by law. This for example would be the case for the ICRC, National Societies of the Red Cross/Red Crescent, the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations World Food Programme (WFP), the International Organization for Migration (IOM), and other Humanitarian Organizations performing a specific task or function in the public interest and which is laid down by law, in so far as the Processing of Personal Data is necessary to accomplish those tasks.⁶³ In this case, the term “necessary” is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,⁶⁴ to fulfil the relevant purpose).

Cases where this legal basis may be relevant include distributions of assistance, where it may not be practicable to obtain the Consent of all the possible beneficiaries, and where it may not be clear whether the life, security, dignity and integrity of the Data Subject or of other people are at stake (in which case “vital Interest” may be the most appropriate legal basis for Processing).

Other scenarios where this legal basis may be relevant include the Processing of Personal Data of persons in detention, where this type of activity is within the mandate of the Humanitarian Organization in question. This may happen, for

⁶³ For example, the ICRC has a mandate under the four Geneva Conventions and Additional Protocol I to act in the event of international armed conflict. The ICRC has a right of humanitarian intervention in non-international armed conflicts: <https://www.icrc.org/en/mandate-and-mission>.

⁶⁴ See example at [Section 3.6: Performance of a contract](#).

example, when the Processing of Personal Data relates to persons deprived of their liberty in an armed conflict or other situation of violence, where the Humanitarian Organization has not yet been in a position to visit the Data Subject deprived of liberty and therefore obtain his/her Consent and, subsequently, if Consent is not considered as a valid legal basis due to the vulnerability of the Data Subjects.



Detainees in the Central Prison, Monrovia, Liberia.

In these cases, too, the Humanitarian Organization should, if possible, ensure that the Data Subjects are aware of the Processing of their Personal Data as soon as possible and that they have sufficient knowledge to understand and appreciate the specified purpose(s) for which Personal Data are collected and processed, and are in a position to object to Processing at any point if they so wish.

3.5 LEGITIMATE INTEREST

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, in particular, where it is necessary for the purpose of carrying out a specific humanitarian activity listed in their mission, and provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. In all of these situations, the term “necessary” is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,⁶⁵ to fulfil the relevant purpose).

⁶⁵ See example at [Section: 3.6 Performance of a contract](#).

Legitimate interest may include situations such as the following:

- The Processing is necessary for the effective performance of the Humanitarian Organization's mission, in cases where important grounds of public interest are not triggered.
- The Processing is necessary for the purposes of ensuring information systems and information security,⁶⁶ and the security of the related services offered by, or accessible via, these information systems, by public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services and by providers of security technologies and services. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems.
- The Processing is necessary for the purposes of preventing, evidencing and stopping fraud or theft.
- The Processing of Personal Data is necessary for the purposes of anonymizing or pseudonymizing Personal Data.⁶⁷
- The Processing is necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial, administrative or any out-of-court procedure.

EXAMPLE:

A Humanitarian Organization processes Personal Data in the course of scanning its IT systems for viruses; verifying the identity of beneficiaries for anti-fraud purposes; and defending itself in a legal proceeding brought by an ex-employee. All these Processing activities are permissible based on the legitimate interest of the organization.

⁶⁶ Information security may include preservation of confidentiality, integrity and availability of information, as well as other properties such as authenticity, accountability, non-repudiation and reliability. See ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

⁶⁷ See [Section 2.3: Aggregate, Pseudonymized and Anonymized data sets](#). Pseudonymization means Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without additional information.

3.6 PERFORMANCE OF A CONTRACT

Under this legal basis Humanitarian Organizations may process Personal Data where it is necessary for the performance of a contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract. Once again, the term “necessary” is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient, to fulfil the relevant purpose).

This will generally be the case with regard to data Processing for the following purposes:

- the management of human resources files, including recruitment
- the management of relations with suppliers of goods/services
- relationships with donors.

EXAMPLE:

A Humanitarian Organization keeps personnel files about its staff in order to fulfil its employment obligations to them. This is permissible in order to perform its contractual employment obligations to its staff. On the other hand, if the same organization has outsourced its data Processing to a Third Party in the same country where its headquarters are located, granting access to its databases to the outsourcing firm will not be regarded as necessary for the performance of its contract with the firm, since the choice to outsource data Processing was a choice of convenience rather than a matter of necessity. In this case it should be considered whether the legitimate interest of the organization would be a suitable legal basis.

3.7 COMPLIANCE WITH A LEGAL OBLIGATION

Under this legal basis, Humanitarian Organizations may process Personal Data where it is necessary to comply with a legal obligation to which Humanitarian Organizations are subject, or to which they submit. This may be the case, for example, in the area of employment law, or for organizations not benefitting from privileges and immunities, if this is necessary to comply with an enforceable legal obligation.

EXAMPLE:

In the country where a Humanitarian Organization operates there is a legal obligation to provide information to the social security and tax authorities about wage payments made to staff. If the organization is subject to domestic jurisdiction, this is permissible based on the legal obligation to which the organization is subject.

However, given the environment in which Humanitarian Organizations operate, the following factors should be taken into account when considering a legal obligation as a basis for the Processing. These will be relevant in particular when authorities require access to Personal Data for law enforcement, intelligence or other purposes:

- existence of the rule of law and separation of powers in the country requiring access to the data
- respect for human rights, including the right to effective judicial redress
- existence of an armed conflict or a situation of violence, where the authority requiring access may represent a party
- the nature of the data, and whether inferences could be made from the data leading to discrimination or prosecution (for example, if names or data relating to food needs reveal religious affiliation or ethnicity, if Health Data reveal sexual orientation in a country where homosexuals are persecuted, or if the Data Subject whose data are being requested faces the death penalty)
- whether the Humanitarian Organization enjoys privileges and immunities, and the obligation is not, therefore, applicable.

In this respect, it is also important to stress that Humanitarian Organizations should consider whether any legal obligation to disclose data applicable to them may put their Data Subjects at risk of discrimination, persecution, marginalization or repression, in which case they should consider not engaging in data collection in the first place.

CHAPTER 4

INTERNATIONAL DATA SHARING

4.1 INTRODUCTION

Humanitarian Emergencies know no borders and regularly create the need for Humanitarian Organizations to share data with other entities across borders to provide the necessary humanitarian response. Accordingly, ensuring efficient cross-border flows of Personal Data between different countries is essential to the work of Humanitarian Organizations. In addition, the adoption of new technologies in humanitarian responses requires the involvement of multiple Data Processors and Sub-Processors which are, almost inevitably, established in various jurisdictions other than that where the Humanitarian Emergency takes place. This may be the case, for example, when cloud-based solutions are used by Humanitarian Organizations to process Personal Data, in which case data may be hosted in the territory where the organization is headquartered, and service providers may be acting as Data Processors and Sub-Processors in a number of jurisdictions.⁶⁸



Nizip refugee camp, near the Syrian border, Gaziantep province, Turkey, November 2016.

As discussed in [Section 2.4: Applicable law and International Organizations](#), some Humanitarian Organizations are International Organizations which enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence. Accordingly, they process Personal Data according to their own rules, which apply across their work irrespective of the territory they operate in, and subject to the control of and

⁶⁸ See [Chapter 10: Cloud Services](#).

enforcement by their own compliance systems. Thus, they constitute their own “jurisdiction”, and data flows within them and their subordinate bodies do not fall within the scope of this Chapter.⁶⁹

The following are just a few examples of entities with which a Humanitarian Organization may need to share data across national borders:

- offices within the same non-governmental organization (NGO) operating in different countries
- other NGOs, International Organizations, and United Nations agencies
- government authorities
- Data Processors such as service providers, consultants or researchers collecting and/or Processing Personal Data on behalf of the Humanitarian Organization
- academic institutions and/or individual researchers
- private companies
- museums.

International Data Sharing includes any act of making Personal Data accessible outside the country where they were originally collected or processed via electronic means, the internet or others. Publication of Personal Data in newspapers, the internet or via radio broadcast usually counts as data sharing if it makes it possible for data to be accessed across borders.

International Data Sharing includes any act that results in Personal Data being transferred, shared or accessed across national borders or with International Organizations. Accordingly, International Data Sharing may involve one of the following situations:

- The Humanitarian Organization transfers data to an organization in another jurisdiction. The receiving entity is a new Data Controller, which determines the means and purposes of Processing.
- The Humanitarian Organization transfers data to an organization in another jurisdiction, but remains the entity which decides on the means and purposes of Processing, and the receiving entity processes Personal Data exclusively according to the instructions of the sharing entity. In this case, the receiving entity is a Data Processor.

Both these scenarios involve a risk that, once Personal Data are shared, they lose some or all of the protection that they enjoyed when they were processed exclusively by the Humanitarian Organization. In both of these scenarios, therefore, it is important to ensure that all reasonable measures are put in place by the sharing organization to avoid unintentional loss of protection.

69 See [Section 2.4: Applicable law and International Organizations](#).

It should not be forgotten that data sharing is a Processing operation and is therefore subject to all the requirements set out in the previous Chapters.⁷⁰ This Chapter explains the additional precautions Humanitarian Organizations should take whenever carrying out International Data Sharing.

4.2 BASIC RULES FOR INTERNATIONAL DATA SHARING

In order to provide protection for International Data Sharing, all of the following steps should be followed:

- Any data protection rules or privacy requirements applicable to the data sharing⁷¹ (including any data protection or privacy requirements of local law, if applicable) have been satisfied prior to the transfer.
- A legal basis must be provided for the transfer.
- An assessment should be carried out to determine whether the transfer presents any unacceptable risks for the individual (e.g. discrimination or repression).
- The organization that initiates the transfer must be able to demonstrate that adequate measures have been undertaken to ensure compliance with the data protection principles set forth in this Handbook by the recipient entity in order to maintain the level of protection of Personal Data with regard to International Data Sharing (accountability).
- The individual should be informed about the recipient(s) of the transfer. The transfer should not be incompatible with the reasonable expectations of the individuals whose data are transferred.

4.3 PROVIDING A LEGAL BASIS FOR INTERNATIONAL DATA SHARING

4.3.1 INTRODUCTION

As mentioned above, this Handbook is designed to assist in the application and respect of data protection principles and rights in humanitarian situations. It does not, however, replace or provide advice on domestic legislation on data protection, where this applies to a Humanitarian Organization not benefitting from the privileges and immunities enjoyed by an International Organization. It should therefore be noted that the considerations covered in this Chapter are in addition to any requirements of local law that may apply in the country from which the data are to be transferred, in so far as they apply to a particular Humanitarian Organization. Dozens of countries in all regions of the world have enacted data protection laws that regulate International Data Sharing; in order to assess such

⁷⁰ See [Chapter 2: Basic principles of data protection](#) and [Chapter 3: Legal bases for Personal Data Processing](#).

⁷¹ See [Chapter 2: Basic principles of data protection](#).

laws, the Humanitarian Organization should consult with its DPO, legal department and/or local legal adviser.

4.3.2 LEGAL BASES FOR INTERNATIONAL DATA SHARING

International Data Sharing may be carried out:

- when the transfer serves the vital interests of Data Subjects or other persons
- for important grounds of public interest, based on the Humanitarian Organization's mandate
- for the legitimate interest of the Humanitarian Organization, based on the organization's declared mission, in cases when this interest is not overridden by the rights and freedoms of the Data Subjects and the Humanitarian Organization has provided suitable safeguards for the Personal Data
- with the Consent of the Data Subject
- for the performance of a contract with the Data Subject.

These legal bases are used in similar ways to their application in Personal Data Processing.⁷² In addition, as International Data Sharing involves additional risks, the factors listed below in the section on "Mitigating the risks to the individual" should be given due consideration.

4.4 MITIGATING THE RISKS TO THE INDIVIDUAL

The following factors are important when carrying out International Data Sharing:

- Risks may be lower if the transfer is to an organization that is subject to the jurisdiction of a country or to an International Organization that has been formally assessed as adequate from a data protection point of view. In general terms, this means that the recipient of data is in a country that has been formally determined to have a regulatory regime for data protection in line with high international standards, including an independent supervisory authority, freedom from mass surveillance and access to judicial redress for individuals. However, only a small number of countries have been found to offer adequate protection in a formal sense by national or regional governmental authorities. This means that relying on an adequacy finding is unlikely to be of use to Humanitarian Organizations in most circumstances. Adequacy is not a prerequisite for International Data Sharing, but is a factor to be taken into account.
- Appropriate safeguards should be used for International Data Sharing, when this is logistically feasible, such as contractual clauses binding the recipient to provide appropriate data protection or checking whether the recipient is committed to complying with a code of conduct on Personal Data protection.
- The Humanitarian Organization should be accountable for the International Data Sharing it engages in.

⁷² See [Chapter 3: Legal bases for Personal Data Processing](#).

These last two factors are considered in more detail below.

EXAMPLE:

A humanitarian NGO has its headquarters in Country X and wants to transfer files containing Personal Data on vulnerable individuals to whom it provides humanitarian services to another NGO in Country Y. The files will be made available by putting them on its secure web-based platform, allowing the organization in Country Y to access them. Country Y has been formally found to provide an adequate level of data protection by the public authorities of Country X. Making the files available on the web-based platform qualifies as International Data Sharing, but the transfer may take place on the basis that there is an adequate level of protection in Country Y, subject to the further considerations set out under Section 4.4.1 Appropriate Safeguards, below.

4.4.1 APPROPRIATE SAFEGUARDS/CONTRACTUAL CLAUSES

One of the measures for a Humanitarian Organization to consider when deciding on the mitigation of the risks involved in International Data Sharing is to ensure that the recipient puts appropriate safeguards in place to protect Personal Data.

In practice, such safeguards may be provided by a legally binding contractual agreement, developed by the Humanitarian Organization itself or adapted from other internationally-recognized sources, by which the organization and the party to which the data are transferred commit to protect the Personal Data in question on the basis of the data protection standards that apply to the Humanitarian Organization.

The European Commission has issued standard contractual clauses for transfers from Data Controllers to Data Controllers and to Data Processors established outside the EU/EEA⁷³ for Humanitarian Organizations subject to EU data protection law or wishing to use these clauses.

Another factor to consider when deciding on risk mitigation is whether the other party involved in data sharing is committed to a code of conduct covering Personal Data Processing⁷⁴ and the extent to which such a code of conduct is applied in practice, whether it is binding and enforceable or not.

⁷³ See European Commission, Model Contracts for the transfer of personal data to third countries: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

⁷⁴ See for example, International Red Cross and Red Crescent Movement Restoring Family Links Network, Code of Conduct on Data Protection: <https://www.icrc.org/en/document/rfl-code-conduct>.

Even when a legal basis exists for the transfer and mitigating measures are put in place, it may not be appropriate to carry out International Data Sharing, because of factors such as the following:

- The nature of the data could put individuals at risk.
- There are good reasons to believe that the parties receiving the data may not be able to ensure that they receive adequate protection.
- The conditions in the country where the data are to be sent make it unlikely that they will be protected.
- The data are being processed on the basis that they are protected by an Organization's immunity from jurisdiction and the receiving organization does not enjoy such immunity.

EXAMPLE:

A Humanitarian Organization that is an International Organization with offices in country X wants to transfer files containing Personal Data on vulnerable individuals to whom it provides humanitarian services to an NGO in the same country. As a transfer from an International Organization to an organization subject to the jurisdiction of X, the sharing constitutes International Data Sharing. The Humanitarian Organization signs standard contractual clauses with the NGO. However, there is a significant danger that an armed group may attack the facilities of the NGO and it has a record of losing data that is sent to it. The Humanitarian Organization should seriously consider not transferring the data, irrespective of contractual clauses being signed.

To identify and address or mitigate such risks properly, a DPIA should be carried out.⁷⁵ In case of doubt, the Humanitarian Organization's DPO should be consulted.

4.4.2 ACCOUNTABILITY

It is important for the Humanitarian Organization that initiates the transfer to be able to demonstrate that adequate and proportionate measures have been undertaken to ensure compliance with basic data protection principles with regard to International Data Sharing. The Humanitarian Organization is accountable to the Data Subject whose data are being shared. This can include measures such as the following:

- keeping internal records concerning data Processing and, in particular, a log of the transfer and a copy of the data transfer agreement made with the party to which the Personal Data is being transferred, if applicable
- appointing a DPO
- drafting Personal Data Processing policies, including a data security policy
- performing and keeping a record of the DPIA(s) relating to the transfer
- registering the transfer with the competent authorities (i.e. data protection authorities), if required by applicable law.

⁷⁵ See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

For any International Data Sharing, appropriate measures should be used to safeguard the transmission of Personal Data to Third Parties. The level of security⁷⁶ adopted and the method of transmission should be proportionate to the nature and sensitivity of Personal Data and to the risks involved. It is also advisable to consider this factor as part of any DPIA to further specify the precautions to be taken.

4.5 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

In the event that a Data Processor is employed by a Data Controller, irrespective of whether the Data Processor is located in a country other than that of the establishment of the Data Controller, their relationship should as much as possible be governed by a binding agreement to protect the Processing of the Personal Data that are shared between them.

A number of issues may have to be clarified in the relevant contractual documents, in order to ensure that Personal Data are properly protected, for example:

- whether the retention policies of the Data Processor are acceptable (e.g. mobile phone operators/financial institutions are subject to domestic data retention requirements)
- what additional types of data are collected by the Data Processor as part of the Processing (e.g. for mobile phone operators, geolocation and other phone metadata)
- whether the Processing of Personal Data by the Data Processor follows the instructions provided by the Data Controller
- how Personal Data are disposed of by the Data Processor after the contracted Processing.

4.6 THE DISCLOSURE OF PERSONAL DATA TO AUTHORITIES

Issues may arise regarding the disclosure and transfer of Personal Data by Humanitarian Organizations to authorities, particularly when they represent a party to a conflict or an actor in other situations of violence. Such disclosure may be problematic for neutral, impartial and independent Humanitarian Action. This is particularly true if disclosure is prejudicial to a Data Subject in view of his/her humanitarian situation, or where such transfers would jeopardize the organization's security or its future access to persons affected by armed conflict or violence, to parties to a conflict, or to information necessary to perform its mandate.

⁷⁶ See [Section 2.8: Data security and Processing security](#).

Humanitarian Organizations enjoying privileges and immunities as International Organizations should ensure that their specific status is respected and refuse to accede to such requests unless necessary in the best interest of the Data Subjects and Humanitarian Action. When a Humanitarian Organization enjoying privileges and immunities needs to transfer data to Humanitarian Organizations that do not enjoy such privileges and immunities, the risk that the recipient may not be in a position to resist such requests should be taken into account. This risk is specifically recognized in the International Conference of Privacy and Data Protection Commissioners' Resolution on Privacy and International Humanitarian Action of 2015:⁷⁷

“Humanitarian organizations 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.”

⁷⁷ International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, 2015. *op. cit.*

CHAPTER 5

DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

5.1 INTRODUCTION

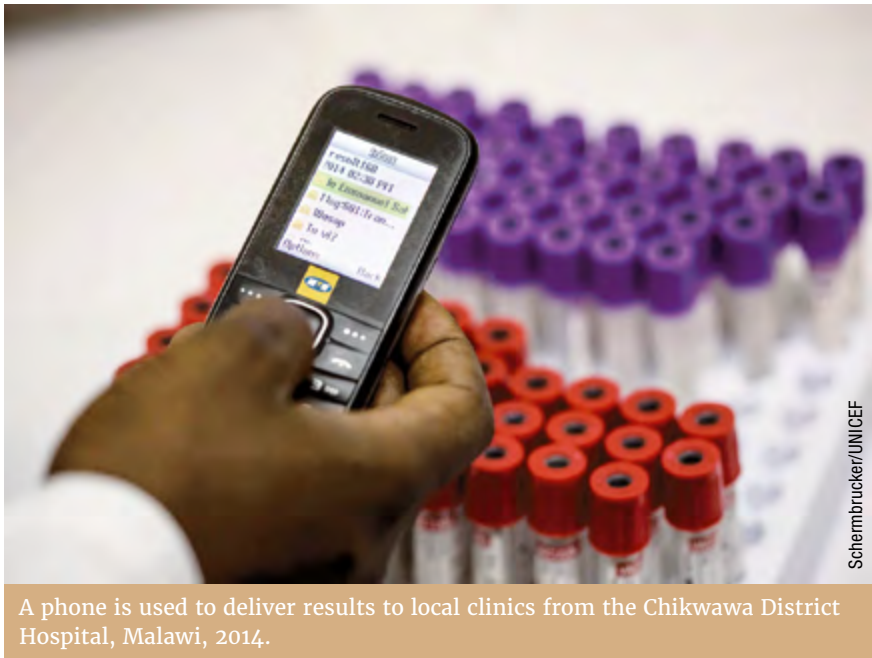
The Processing of Personal Data can increase risks for individuals, groups and organizations, as well as society as a whole. The purpose of a Data Protection Impact Assessment (DPIA)⁷⁸ is to identify, evaluate and address the risks to Personal Data – and ultimately to the Data Subject – arising from a project, policy, programme or other initiative. A DPIA should ultimately lead to measures that contribute to the avoidance, minimization, transfer or sharing of data protection risks. A DPIA should follow a project or initiative that requires Processing of individuals' data throughout its life cycle. The project should revisit the DPIA as it undergoes changes or as new risks arise and become apparent.

Here are examples of when a DPIA is appropriate:

- The offices of the Humanitarian Organization have been looted once too often. It wants field offices either to dispose of their paper files or send them to headquarters and to rely instead on a cloud-based storage system. Should field offices do away with paper, CDs and flash drives?
- A local NGO or authority approaches a Humanitarian Organization saying it wants to reunite families split apart because of violence in the country. It wants the Humanitarian Organization to supply all the information it has on missing persons in the country. Should the information be shared? If so, how much personal information should be shared in order to trace missing persons? Under what conditions should personal information be disclosed to a host government?
- A tsunami sweeps away dozens of coastal villages. Thousands are reported missing. How much personal information should the Humanitarian Organization collect from the families of persons unaccounted for? Should it be a lot or a little? Should it include information on health or genetic data, religious affiliation or political views which, if disclosed, could give rise to significant harm to the individuals?
- Should Humanitarian Organizations publish pictures of unaccompanied children unaccounted for on the internet? Should the Humanitarian Organization produce posters? Under what circumstances?

The DPIA can play a key role in determining who might be adversely affected by the privacy or data protection risks and how they might be harmed.

⁷⁸ The authors express their gratitude to Trilateral Research for permission to use the material on Data Protection Impact Assessments.



A phone is used to deliver results to local clinics from the Chikwawa District Hospital, Malawi, 2014.

This Chapter is a step-by-step guide for Humanitarian Organizations on how to conduct a DPIA and what should be included in a DPIA report. Appendix I contains a template for a DPIA report.⁷⁹ Although a DPIA report is not the end of a DPIA process, it is crucial to its success. It helps the Humanitarian Organization identify the privacy impacts of a proposed project and what must be done to ensure that the project protects Personal Data. It also helps the Humanitarian Organization reassure stakeholders that it takes their rights to privacy and data protection seriously and that it seeks the views of those who might be affected by or interested in the programme. Humanitarian Organizations should consider making the DPIA report or, at least, a summary of it available to stakeholders.

⁷⁹ See [Appendix I: Template for a DPIA report](#).

5.2 THE DPIA PROCESS

This section provides a guide through the steps necessary to undertake a DPIA. There are different approaches to conducting DPIAs. The following guidance draws on best practices from a range of sources.⁸⁰

5.2.1 IS A DPIA NECESSARY?

Any organization that collects, processes, stores and/or transfers Personal Data to other organizations should consider conducting a DPIA, the scale of which will depend on how seriously the organization assesses the risks. A Humanitarian Organization may not be aware of all the data protection risks beforehand, some of which may only become apparent during the course of the DPIA. The Humanitarian Organization may view the risks as being so small that they do not justify a DPIA. Some risks may be real, but still relatively small, so the DPIA process and report may be correspondingly short. Other risks may be very serious and the Humanitarian Organization will want to conduct a thorough DPIA. There is no one-size-fits-all solution.

5.2.2 THE DPIA TEAM

The second step involves identifying the DPIA team and setting the terms of reference. The DPIA team should include or consult the Humanitarian Organization's DPO. Depending on the scale of the DPIA to be undertaken, the DPIA team could include experts from the Humanitarian Organization's IT, legal, operations, protection, policy, strategic planning, archives and information management, and public relations groups. The team undertaking the DPIA should be familiar with data protection requirements as well as the Humanitarian Organization's confidentiality rules and codes of conduct. Importantly, it should also include members familiar with the planned project. Setting the terms of reference includes planning the time frame for the DPIA, the scope of the DPIA, the stakeholders to be consulted, the budget for the DPIA, and the steps that will be taken after the DPIA in terms of review and/or audit.

80 David Wright, "Making Privacy Impact Assessment More Effective", *The Information Society* (Vol. 29, No. 5, 2013), pp. 307–315; Office of the NSW Privacy Commissioner, *Guidance. Guide to Privacy Impact Assessments in NSW*, October 2016, Sydney, NSW, Australia; Secretariat of ISO/IEC JTC 1/SC 27; *Information technology – Security techniques – Privacy impact assessment – Methodology*, ISO/IEC nth WD 29134:2017, 23 October 2014: <https://www.iso.org/standard/62289.html>.

5.2.3 DESCRIBING THE PROCESSING OF PERSONAL DATA

The DPIA team should prepare a description of the programme or activity to be assessed. The description should include:

- the aims of the project
- the scope of the project
- linkages with other projects or programmes
- the team responsible for the programme or activity
- a brief description of the type of data that will be collected.

Mapping data flows is a key step of any DPIA. In mapping the information flows of a particular programme or activity, the DPIA team should consider the following questions:

- What type of Personal Data is being collected, from whom and why?
- How will that data be used, stored or transferred?
- Who will have access to the Personal Data?
- What security measures are in place to protect the Personal Data?
- For how long will that data be retained or when will they be deleted? Have different layers of data retention been identified? This can include steps such as (1) storing data deemed sensitive for up to X days, (2) pseudonymizing data then storing the data for a longer time period, and finally (3) full deletion of the data.
- Will the data undergo any cleansing or Anonymization to protect sensitive information?

5.2.4 CONSULTING STAKEHOLDERS

Identifying stakeholders is an important part of conducting a DPIA. Stakeholders include anyone who is interested in or affected by a data protection risk. Stakeholders may be internal and/or external to an organization. The need and value of consulting external stakeholders will depend on how serious the Humanitarian Organization considers the risk to be. For a Humanitarian Organization, consulting stakeholders is a way of identifying risks and/or solutions it may not have considered. It is also a way of raising awareness about data protection and privacy issues. The views of stakeholders should be taken into consideration in the DPIA report and recommendations. In order for consultation to be effective, stakeholders should be provided with sufficient information about the programme and given the opportunity to express their views. There are different ways to engage stakeholders, so the DPIA team should determine the most appropriate one depending on the programme or activity.

5.2.5 IDENTIFY RISKS

One way to identify risks is to create a spreadsheet listing privacy principles, threats to those principles, vulnerabilities (susceptibility to the threats), and risks arising from the threats and vulnerabilities. A threat without a vulnerability or vice versa is not a risk. A risk arises when a threat acts to exploit a vulnerability.

5.2.6 ASSESS THE RISKS

A data protection risk assessment addresses the likelihood or probability of a certain event and its consequences (i.e. impacts). One can assess the risks by undertaking one or more of the following steps:

- Consult and deliberate with internal and/or external stakeholders to identify risks, threats and vulnerabilities.
- Evaluate the risks against agreed risk criteria.⁸¹
- Assess the risk in terms of likelihood and severity of impact.
- Assess against the necessity, suitability and proportionality tests.

5.2.7 IDENTIFY SOLUTIONS

This step involves developing strategies to eliminate, avoid, reduce or transfer the privacy risks. These strategies could include technical solutions, operational and/or organizational controls and/or communication strategies (e.g. to raise awareness).

5.2.8 PROPOSE RECOMMENDATIONS

The DPIA team should produce a set of recommendations based on the outcome of the previous steps. Recommendations may include a set of solutions, changes at the organizational level, and potentially changes to the Humanitarian Organization's overall data protection strategy or that of the programme. A set of recommendations should be included in the DPIA report.

5.2.9 IMPLEMENT THE AGREED RECOMMENDATIONS

The DPIA team should prepare a written report on the considerations and findings of the DPIA. As organizations will need to conduct DPIAs regularly, the length and level of detail of a DPIA report will vary greatly. For example, if an organization is considering publication of Personal Data for research purposes, it should produce documentation reflecting the full details of its data protection impact analysis. Conversely, an organization that is deciding whether to switch from using one brand of word-processing software to another should consider data protection issues, given that the software will be used to process personal information, but a detailed DPIA may not be necessary (unless the software involves new data flows in a cloud environment).

⁸¹ For definitions of risk terms, see ISO/Guide 73:2009(en) *Risk management – Vocabulary*: <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en>.

In addition to documenting and implementing data protection decisions, a Humanitarian Organization should consider whether it would be useful to Data Subjects or to the public to understand the considerations underlying its data protection decision-making. Accordingly, the organization might then share the report (in whole or in part) with relevant stakeholders and thereby show that it takes data protection seriously. Sharing the DPIA report also may be a way of raising awareness and inviting further comments or suggestions from stakeholders. However, in some cases, the Humanitarian Organization may decide against sharing the DPIA report if it contains sensitive information (e.g. for reasons of physical security, continuity of operations, access, etc.). In such cases, the Humanitarian Organization could consider sharing a summary of the DPIA report or a redacted version.

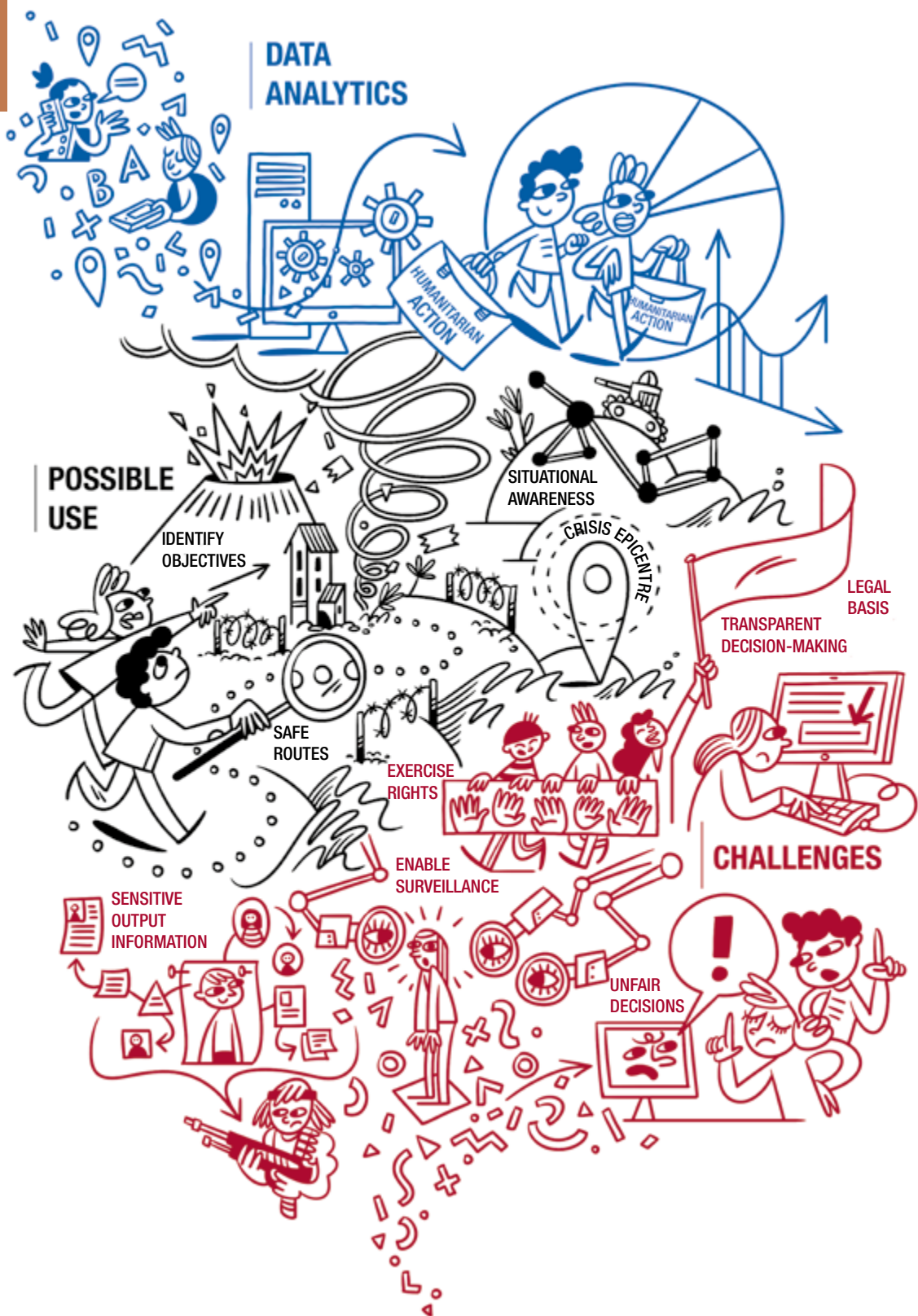
5.2.10 PROVIDE EXPERT REVIEW AND/OR AUDIT OF THE DPIA

Humanitarian Organizations should ensure that a data protection expert, such as the organization's Data Protection Officer or his/her staff, reviews or audits the implementation of the DPIA. In the interest of an accurate audit, the DPIA report must contain a methodology section.

5.2.11 UPDATE THE DPIA IF THERE ARE CHANGES IN THE PROJECT

The Humanitarian Organization should update the DPIA if the activity covered by it changes in some significant way or if new data protection risks emerge.

DATA ANALYTICS



CHAPTER 6

DATA ANALYTICS AND BIG DATA

6.1 INTRODUCTION

As Humanitarian Action is driven by information;⁸² performing Data Analytics through Personal Data Processing has potentially significant benefits for Humanitarian Organizations. The term “Data Analytics” denotes the practice of combining very large volumes of diversely-sourced information (Big Data) and analysing them, using sophisticated algorithms to make informed decisions. Big Data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on the possibility of analysing, understanding and taking advantage of the full value of data (in particular using Data Analytics applications). For the purposes of this chapter the two terms, “Data Analytics” and “Big Data”, will be used interchangeably.

Data Analytics may be used for objectives such as identifying potential threats relevant to Humanitarian Action, enhancing preparedness, identifying individuals or categories of individuals in need, or predicting the possible patterns of evolution of contagious diseases, conflicts, tensions and natural disasters.

Data Analytics may significantly enhance the effectiveness of work carried out by Humanitarian Organizations. In particular, benefits may include mapping or identifying:

- patterns of events in Humanitarian Emergencies involving protected persons in conflicts or other situations of violence
- the spread of diseases or natural disasters, thus predicting possible developments and preparing for them to prevent harm
- the epicentre of a crisis
- safe routes
- individual humanitarian incidents
- vulnerable individuals or communities who are likely to require humanitarian response
- matches in cases of families separated in a Humanitarian Emergency.

Consequently, it is possible to identify two broad categories of applications for the use of Data Analytics in humanitarian situations. Firstly, applications which recognize general patterns and secondly, those aimed at identifying individuals or groups of individuals of relevance for Humanitarian Action.

82 United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Humanitarianism in the Age of Cyber-Warfare* (OCHA Policy and Studies series, 2014).



Mobile phone data from West Africa were used to map population movements and predict how the Ebola virus might spread.

The use of Data Analytics has often given rise to accusations of misleading and inaccurate results; justifying arbitrary and automated decisions that do not take case-specific particularities into consideration; generating data that may be used to enable more effective surveillance through digital footprints; and the possibility of breaching anonymity through reverse engineering, therefore leading to re-identification of individuals included in the Processing. The data protection implications of Big Data were highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Big Data, adopted in Mauritius in 2014.⁸³

Concerns may also be raised when applying basic data protection principles to Data Analytics, for instance with regard to 1) purpose specification insofar as Data Analytics Processing uses Personal Data for previously unforeseen purposes; 2) transparency requirements, given that not much information is typically provided to Data Subjects; or 3) the principle of legitimate Processing, which is not always easily identifiable as a suitable legal basis for the Processing.⁸⁴

This chapter aims to provide guidance for Humanitarian Organizations engaging in Data Analytics activities. It explains how Data Analytics can be performed in accordance with data protection principles and identifies potential challenges.

⁸³ International Conference of Data Protection and Privacy Commissioners, Resolution on Big Data, Fort Balaclava, Mauritius, 2014: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf?mc_phishing_protection_id=28047-br1tehqu81eaoar3q10.

⁸⁴ See [Chapter 2: Basic principles of data protection](#).

Several data protection-related specificities need to be highlighted at the outset of this analysis:

- *Data sources.* First of all, it is important to identify the source of data. Much Data Analytics Processing undertaken by Humanitarian Organizations is based on publicly available data, such as information from government agencies or public records, social media networks, census data and other publicly available demographic and population surveys. In other cases, Humanitarian Organizations may partner with private enterprises such as telecommunications or infrastructure companies, internet services, healthcare providers or other commercial organizations to improve the humanitarian and disaster response.
- *Emergency response.* Although the outputs from Data Analytics have irrefutable benefits for Humanitarian Organizations, they may not always be used for an ongoing emergency or to address the vital interests of the individuals concerned. There may, for example, be cases where Data Analytics Processing takes place after an incident has occurred and has been dealt with, to support administrative work or to contribute to strategies to improve the response to future emergencies.
- *Accuracy.* Data used for analytics may not always be representative and accurate and may contain bias, which can lead to incorrect results.⁸⁵ Working on anonymized or aggregated data, while potentially less intrusive vis-à-vis the privacy of the individuals involved, may increase this risk.
- *Automated decision.* Data Analytics with no human intervention or contextual background can also lead to incorrect insights and decisions.⁸⁶
- *Reuse of data for other purposes.* The use of Big Data often poses questions about whether Personal Data can be used for purposes other than those for which they were collected. This raises questions under data protection law, which generally requires that Personal Data be collected for defined purposes and processed for such purposes or for compatible purposes only, and not reused for other purposes without the Consent of the individual concerned or some other legal basis.
- *The sensitivity of data output created by Personal Data Processing in humanitarian situations.* It is important to understand that otherwise publicly available data, for instance data on social media networks and data not generally considered as sensitive, may generate Sensitive Data when processed for Data Analytics purposes in a humanitarian situation. This can happen when Processing anodyne data enables the profiling of individuals which could

⁸⁵ UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report, p. 12: http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_o.pdf.

⁸⁶ *ibid.*, p. 12: “Data typically must be representative in order to accurately inform insights. Therefore, it is important to consider that certain data sets or algorithms may contain biases. To avoid biases, data quality, accuracy and human intervention in any of the data processing activities are crucial.”

result in discrimination or repression, such as, for example, potential victims, people affiliated with a particular group in a situation of violence, or bearers of a particular illness. In these cases, *data smoothing* can be a valuable way to protect individual and group privacy while allowing access to data.⁸⁷ However, it is important to note that as data are temporally and spatially *smoothed*, the clarity of findings is also diminished.

- *Anonymization*. Doubts may exist as to the effectiveness of Personal Data Anonymization and the possibility of re-identification in Data Analytics operations, regardless of whether for humanitarian or other purposes. Again, data smoothing can complement Anonymization to provide another layer of protection to prevent re-identification.
- *Regulatory fragmentation*. While many states have enacted data protection law and many Humanitarian Organizations have already implemented data protection policies and guidelines, the question of how specifically Big Data are regulated across borders at times of humanitarian crises remains open.⁸⁸

It is important to realize that when Data Analytics are used for Humanitarian Action, the implications for individuals may be far more serious than in other settings (e.g. Data Analytics performed in a commercial environment). For example, even when the analysed data have been anonymized, the results may have severely negative consequences not only for individuals but also for groups of individuals. Humanitarian Organizations should consider whether any data they release or conclusions they draw from Data Analytics may be used, even in the aggregate, to target the people they seek to protect. Furthermore, such potentially affected groups of individuals do not always include the Data Subjects. In many cases invisible populations can suddenly become visible by being separated from the group identified by the data set.⁸⁹ It is important, therefore, always to keep in mind the “big picture” of the potential implications of Data Analytics on vulnerable individuals.

EXAMPLE:

The extraction and analysis of tweets and other material on social media networks to locate the epicentre and flows of public demonstrations to avoid loss of human life and publication of the findings to authorities may lead to subsequent use of these findings by the same authorities to identify individuals who took part in such public demonstrations (or who did not), which can have severe consequences for the identified groups of individuals.

⁸⁷ Data smoothing means to remove noise from a data set so that important patterns stand out.

⁸⁸ UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report, pp. 7–9, *op. cit.*

⁸⁹ *ibid.*, p. 12.

Data Analytics may involve Processing scenarios such as the following:

EXAMPLE 1: The extraction and analysis of public communications through social media, search engines or telecommunications services, as well as news sources in order to demonstrate how methods including sentiment analysis, topic classification and network analysis can be used to support public health workers and communication campaigns.

EXAMPLE 2: Development of interactive data visualization tools during a humanitarian incident in order to demonstrate how communications signals or satellite data could support emergency response management.

EXAMPLE 3: Analysis of messages received through a Humanitarian Organization's citizen reporting platform.

EXAMPLE 4: Analysis of social media, mobile phone network metadata and credit card data to identify individuals likely to be at risk of enforced disappearance or to locate persons unaccounted for.

The following data sets may be relevant:

- public data sets (i.e. data sets that are already publicly available, such as public records released by governments or information people have intentionally made public in news media or on the internet, including through social media)
- data sets held by Humanitarian Organizations (e.g. lists of distribution beneficiaries, patients, protected individuals, individuals unaccounted for/their families, individuals reporting violations of international humanitarian law/human rights)
- data sets held by private Third Parties (e.g. mobile, telecommunications, banking and financial providers, internet service providers and financial transactions data, remote sensor data, whether aggregated or anonymized or not)
- a combination or aggregation of data sets of Humanitarian Organizations, authorities and/or corporate entities (including organizations mentioned above).

Humanitarian Organizations may play the following roles in data Processing:

- processing data held within their respective organizations (as Data Controllers)
- employing Data Processors (i.e. commercial entities who will perform the Data Analytics on the data held by the Humanitarian Organization)
- requesting commercial entities who are and remain the Data Controller to carry out analytics on data for humanitarian purposes, and provide conclusions/findings to the Humanitarian Organization. Such conclusions could involve either aggregated/anonymized data, or data identifying individuals of possible relevance for Humanitarian Action
- sharing data sets with other Humanitarian Organizations, public authorities and/or commercial entities as joint Data Controllers and/or Data Processors.

These scenarios can be presented as follows:

	Data held by Humanitarian Organizations	Data held by Third Parties (authorities/corporations)
Humanitarian Organization is the Data Controller	Humanitarian Organization may carry out analytics independently, or seek the services of an external Data Processor	External partner provides data to the Humanitarian Organization to process
Third party is the Data Controller	Humanitarian Organization provides data to external partner to process	At the request of the Humanitarian Organization the external partner processes data

It is important to note that the Humanitarian Organization and the Third Party may both have the two roles of Data Controller and Data Processor at the same time. For instance, data may be held by a Third Party organization, be processed by the Third Party organization at the Humanitarian Organization’s behest and then subsequently be shared by the Humanitarian Organization with other stakeholders.

6.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

Processing Personal Data for Data Analytics presents important challenges for individual data protection. When the Processing uses large data sets that are processed for purposes other than those for which they were collected, it risks violating basic notions of data protection, including purpose limitation, data minimization or the retention of data for only as long as necessary for execution of the purposes of collection. In essence, Data Analytics thrive in open and unrestricted Processing environments while, on the other hand, Personal Data protection favours limited and well-defined Personal Data Processing. It is for this reason that data protection needs to be applied innovatively to Data Analytics.⁹⁰

The basic principles of data protection constitute the baseline to be respected while engaging in Data Analytics Processing. As mentioned in [Chapter 2: Basic principles of data protection](#), the basic data protection principles that need to be respected while undertaking Data Analytics include the principle of the fairness and lawfulness of the Processing; the principle of transparency; the purpose limitation principle; the data minimization principle; and the data quality principle. While some of these principles are compatible with the purposes of Data Analytics, others may raise questions or conflicts, and consequently special care must be taken by

⁹⁰ European Data Protection Supervisor (EDPS), Opinion 7/2015, *Meeting the challenges of big data*, 19 November 2015, p. 4: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

Humanitarian Organizations when applying them in practice. Other Humanitarian Organizations have developed principles for handling Big Data that complement the discussion in the present Chapter.⁹¹

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

One of the most significant challenges in humanitarian Data Analytics is that analytics operations are most likely to be run on existing data sets, previously collected by the Humanitarian Organization or Third Parties for a different purpose. The key question is, therefore, to determine whether the envisaged analysis is compatible with the original purpose of collection. If so, the analytics operation can be run under the existing legal basis. If not, a new legal basis for subsequent Processing needs to be found.

6.2.1 PURPOSE LIMITATION AND FURTHER PROCESSING

As discussed in [Chapter 2: Basic principles of data protection](#), at the time of collecting data the Humanitarian Organization concerned must determine and set out the specific purpose/s for which data are processed. The specific purpose/s should be explicit and legitimate and could include anything from restoring family links, to protecting individuals in detention, forensic activities or protecting water and habitat. Ideally, the purpose of any envisaged analytics should be specified at the outset of data collection.

With regard to Further Processing, irrespective of the legal basis used for the initial Processing, Humanitarian Organizations may process Personal Data for purposes other than those initially specified at the time of collection where the Further Processing is compatible with those purposes, including where the Processing is necessary for historical, statistical or scientific purposes.⁹²

Data Analytics Processing operations may frequently require Processing data for purposes other than those for which they were initially collected. However, the purposes of Data Analytics will rarely be foreseeable at the time of initial Personal Data collection.

In order to establish whether the analytics operation can be considered Further Processing that is compatible with the purpose for which the data were initially collected, attention should be given to the following factors:

⁹¹ See United Nations Global Pulse, Privacy and Data Protection Principles: <http://www.unglobalpulse.org/privacy-and-data-protection-principles>; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data, January 2017: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>.

⁹² See [Section 2.6.3: Further Processing](#).

- any link between the purposes for which the data were collected and the purposes of the intended Further Processing
- the situation in which the Personal Data were collected and, in particular, the relationship between Data Subjects and the Data Controller, and possible expectations of the Data Subjects
- the nature of the Personal Data
- the possible consequences of the intended Further Processing for Data Subjects
- the existence of appropriate safeguards.

In considering the above factors, the humanitarian purpose of the data Processing should be kept in mind. In general, humanitarian purposes are likely to be compatible with each other. In cases where Third Party data are processed for purposes that go beyond those for which they were originally collected, due to the humanitarian value in the use of the data sets, there is a case for the data to be used for humanitarian purposes as compatible Further Processing, so long as it does not expose the Data Subjects to new risks or harm, as explained further below. New Processing would not be compatible, even for humanitarian purposes, if new risks arise, or if the risks for the Data Subject outweigh the benefits of Further Processing. Compatibility depends on the circumstances of the case. Further Processing would also not be compatible if Processing is potentially detrimental to the interests of the person to whom the information relates or his/her family, in particular when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty, or their reputation. This includes consequences such as:

- harassment or persecution by authorities or Third Parties
- judicial prosecution
- social and private problems
- limitation of liberty
- psychological suffering.

EXAMPLE 1: Data sets collected by a Humanitarian Organization while dealing with an incident, for instance in order to distribute aid, may be used at a later stage for the purpose of understanding patterns of displacement and pre-deploying aid in subsequent Humanitarian Emergencies.

EXAMPLE 2: Data sets collected by a telecommunications provider in the course of providing its services to its subscribers may not be used without these subscribers' Consent in Data Analytics Processing by Humanitarian Organizations, if it can result in such individuals being profiled as potential bearers of a disease, with consequent restrictions on movement imposed by authorities. In these cases, Humanitarian Organizations and their Third Party counterparts should consider whether mitigating measures, such as data aggregation, would be sufficient to remove the risk identified.

6.2.2 LEGAL BASES FOR PERSONAL DATA PROCESSING

If the purposes of analytics are deemed to be incompatible with the original purpose of Processing, a new legal basis for the analytics should be found. In using Data Analytics, Humanitarian Organizations could process Personal Data based on one or more of the following:⁹³

- the vital interest of the Data Subject or of another person
- the public interest, in particular based on an Organization's mandate under national or international law
- Consent
- a legitimate interest of the Organization
- the performance of a contract
- compliance with a legal obligation.

The use of Consent poses problems for Data Analytics, which are performed on Personal Data that have already been collected and organized in pre-existing data sets. In addition, it may be difficult at the time of collection to ensure that Data Subjects fully appreciate the risks and benefits of Data Analytics, due to the complexity of the Processing operation and implications that may not be fully clear at that stage.

Data Analytics offered by social media networks or mobile phone operators to assist Humanitarian Organizations could, in some cases, be based on Consent, if the social media platform or mobile operator in question is able to inform the Data Subjects of the intended Processing by way of a pop-up window or text message with the relevant information and Consent request. In this scenario, however, if some pockets of individuals withhold Consent the implications for the accuracy of the analytics and consequent conclusions should be considered.

In order to ensure Consent is properly informed, the information provided should take into account the outcome of the DPIA (if one has been completed)⁹⁴ and might also be given via an interface which simulates the effects of the use of data and its potential impact on the Data Subject, in a learn-from-experience approach.⁹⁵ Data Processors should provide easy and user-friendly technical ways for Data Subjects to withdraw their Consent and to react to data Processing incompatible with the initial purposes.⁹⁶

It is important to assess the validity of Consent even when adequate information has been provided to the Data Subjects at the time of collection and the purpose

⁹³ See [Chapter 3: Legal bases for Personal Data Processing](#).

⁹⁴ See [Section 6.7: Data Protection Impact Assessments](#).

⁹⁵ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*, January 2017, *op. cit.*

⁹⁶ *ibid.*

of Further Processing is compatible. This assessment should take into account the Data Subject's level of literacy as well as the risks and harms to the Data Subjects for the Processing of their data.⁹⁷

Where Consent cannot be obtained from the individual providing the data or the Data Subject, Personal Data can still be processed if it is established that it is in the vital interest of the Data Subject or of another person, i.e. where data Processing is necessary in order to protect an interest which is essential for the Data Subject's life, integrity, health, dignity or security or that of another person or group of people. Furthermore, additional legal bases, such as public interest, the legitimate interest of the organization, and performance of a contract or compliance with a legal obligation could be grounds for the Processing.

Regarding the use of vital interest as a legal basis for Humanitarian Organizations' emergency work in armed conflicts and other situations of violence, there are several cases where there is a presumption that the Processing of data by Humanitarian Organizations is in the vital interest of a Data Subject or another person (for example, if data are processed in cases of Sought Persons, or if there are imminent threats against the physical and mental integrity of the persons concerned). However, the condition of vital interest may not be met when data Processing is undertaken in a non-emergency situation, for instance for administrative purposes.

EXAMPLE:

When Data Analytics is undertaken for administrative or purely research purposes, the legal basis of vital interest is not applicable.

Humanitarian Organizations should carefully assess when important grounds of public interest are triggered that they are sufficiently closely linked with the analytics operation envisaged to be used as a lawful basis for the Personal Data Processing. The public interest approach could constitute the suitable legal basis for Data Analytics Processing where a mandate to carry out Humanitarian Action is established in national, regional or international law and where no Consent was obtained and no emergency existed that could invoke vital interest as a legal basis.

Humanitarian Organizations should be aware that public interest as a legal basis for Personal Data Processing is not transferable, because it is specific to the Organization's mandate under national or international law. The conditions (if any) under which a Third Party may undertake the Data Analytics Processing on the Organization's behalf or that are applicable to International Data Sharing need to be examined separately.

⁹⁷ United Nations Development Programme (UNDP), UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*: <http://www.unglobalpulse.org/privacy/tools>.

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. Such legitimate interests may include Processing necessary to make their operations more effective and efficient, including facilitating logistics to enable pre-deployment of aid and staff in anticipation of Humanitarian Emergencies, where such insights could be obtained from data analysis. Data Analytics Processing for administrative purposes may also fall under this category.

EXAMPLE:

Humanitarian Organizations may engage in Data Analytics Processing on their employees' data in order to build up a database of potential staff per region.

Legitimate interests may also be used by commercial entities willing to carry out Data Analytics to assist Humanitarian Organizations where the purpose of the Processing is exclusively humanitarian.

6.2.3 FAIR AND LAWFUL PROCESSING

To be fair and lawful the Processing requires a legal basis, as detailed in [Section 2.5: Data Processing principles](#).

Data Analytics deals in possible correlations, rather than objectivity, and therefore raises numerous questions about the fairness of the Processing, including concerns about sampling, representation and population estimates. Researchers should take care to understand the representativeness of the sample data, attempt to use broad and representative data sets, and report potential biases. Moreover, policymakers should account for these biases when making decisions. When used in policy making, basing analytics on inaccurate data and misinterpretations of findings could lead to harmful and/or unfair policy decisions, or Data Subjects may find themselves affected by potentially biased automated decisions and by generalizations.

In addition, the fairness requirement in data protection law is generally focused on the provision of information, transparency and the impact of the Processing. In Data Analytics, given the complexity of the Processing and the difficulty in performing a meaningful risk analysis, transparency about methodology (including where possible the algorithm) is very important, so that the rigour of the approach can be independently assessed, above and beyond the Data Subjects' right of information.⁹⁸ Care should be taken in decision-making processes about transparency if transparency conflicts with data sensitivity at the individual level, or when transparency in Processing could encourage gamification of the data Processing system by malicious actors and therefore bias it.

⁹⁸ See [Section 6.3: Rights of Data Subjects](#) and [Section 6.5: International Data Sharing](#).

The principle of fairness implies that an assessment of the risks of re-identification should be carried out before de-identification and, where possible, the Data Subject or relevant stakeholders be informed of the results of the assessment. If there is a strong possibility of re-identification, a decision should be taken not to perform the analytics or to adjust the methodology. The proper assessment of such a Data Analytics situation requires the performance of a DPIA.⁹⁹

It is also important that any employees, contractors or other parties involved in Data Analytics undergo training to educate them about the data protection risks and ethical research procedures, and that steps are taken to mitigate those risks.

6.2.4 DATA MINIMIZATION

The data processed by Humanitarian Organizations should be adequate and relevant for the purposes for which they are collected and processed. In particular, this means ensuring that data collection is not excessive and that the time period for which the data are stored, before being anonymized or archived, is limited to the minimum necessary. The amount of Personal Data collected and processed should, ideally, be limited to what is necessary to fulfil the specified purpose(s) of data collection, data Processing or compatible Further Processing, or to what is justified on another legal basis.

On the other hand, Data Analytics typically requires large data sets that include as much information as possible spanning a significant period of time in order to achieve optimum results. This contradicts the data minimization principle, which requires, as discussed above, keeping the contents of data sets collected by Humanitarian Organizations to the absolute minimum for the purposes of the Processing at the time of collection. Therefore, it is important that the purpose of data collection is stipulated as specifically as possible and any retention of data beyond the original project's needs is justified by compatible Further Processing.

In addition, while archived or anonymized data sets may also be used in Data Analytics operations, their use presents technical and legal challenges. With regard to the former, the capacity to process may be hindered by archiving restrictions, while with regard to the latter, special care needs to be taken in order for the outcome of the Processing not to enable re-identification of individuals who were otherwise de-identified. Questions should also be asked about the accuracy of Data Analytics outputs when Processing anonymized or aggregated data. The methods and level of Anonymization or aggregation should therefore be carefully selected to minimize the risks of re-identification and ensure that the data remain of the right quality and utility to achieve credible results.

⁹⁹ See [Section 6.7: Data Protection Impact Assessments](#).

Data Controllers and, where applicable, Data Processors should carefully consider the design of their data analysis, in order to minimize the presence of redundant and marginal data.¹⁰⁰

Personal Data should be retained only for a defined period as necessary for the purposes for which they were collected. Following the initial retention period an assessment should be made as to whether the data should be deleted or whether they should be kept for a longer period to achieve the purpose. Any potential Data Analytics operations should be covered in detail in the relevant retention policy or information notice. If the Processing for Data Analytics is planned at the time of collection, this should be included in the initial information notice, and the retention period envisaged should cover the amount of time required to perform the analytics operation.

If this Processing is performed on pre-existing data sets, as “compatible Further Processing”,¹⁰¹ the Processing should take place within the data retention period allowed for the purpose of initial collection. Renewal of the initial retention period, if a renewal is contemplated by the retention policy at the time of collection, can take place to enable analytics as “compatible Further Processing”.

If the Processing takes place on existing data sets and its Data Analytics purpose is not deemed to be compatible with the purpose of initial collection, a new legal basis for Processing should be found and a specific information notice should be produced explaining the analytics operation and including the retention period.

6.2.5 DATA SECURITY

In considering the suitability of security measures required to protect information in Data Analytics operations, it is important to take into account that the outputs of the Processing, which may correlate and analyse existing data sets, may produce data that are more sensitive than the initial data sets. The outputs, which may include individual or group profiling, could prove harmful to the individuals concerned if they fall into the wrong hands.

In this case, the Humanitarian Organization undertaking the Data Analytics should implement adequate security measures to protect the output, which are appropriate for the risks involved.¹⁰² Additionally, regular data security and data privacy training is essential to raise awareness of security threats and to avoid Data Breaches.

¹⁰⁰ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*, January 2017, *op. cit.*

¹⁰¹ See [Section 2.6.3: Further Processing](#).

¹⁰² See [Section 6.2.5: Data security](#) and [Section 2.8: Data security and Processing security](#).

6.3 RIGHTS OF DATA SUBJECTS

The rights of the Data Subjects are described in [Section 2.11: Rights of Data Subjects](#). The rights to information, access, correction, erasure and objection are considered crucial components of an effective data protection policy. However, the Processing of Personal Data for Data Analytics poses significant challenges.

The Data Subject's exercise of the right to information (also relevant to the transparency principle, see [Section 6.2.1: Purpose limitation and Further Processing](#)) is more difficult with Data Analytics, as it is not always possible to provide detailed information on the Processing directly to the individuals concerned, particularly when Processing takes place on existing data sets. It is therefore important to explore alternative means of information provision, for example, by using the websites of the organizations involved, other internet platforms likely to be used by the Data Subjects, or other means of mass communication (e.g. newspapers, leaflets or posters). Where the provision of information to Data Subjects proves difficult or impossible, the creation of a national or cross-national information resource (easier to be found than websites of single operators) has been suggested. It may also be advisable to investigate providing information to group representatives.

Organizations engaged in humanitarian Data Analytics are encouraged to incorporate complaint procedures into their Personal Data Processing practices and internal data protection policies. These procedures should enable data correction and erasure. However, it should be recognized that the exercise of certain individual rights may be limited by the legal basis of the Processing. For example, requests for opt-outs by individuals may not be observed in the event of Processing undertaken under the legal basis of public interest described above.

Humanitarian Organizations need to ensure that no automated decisions are taken with regard to individuals which could lead to harm or exclusion from humanitarian programmes, without any human intervention. In practice, this means that a human being should always be the final decision-maker when decisions are taken on the basis of Data Analytics outputs that may have adverse effects on individuals.

EXAMPLE:

In the event of aid distribution, a decision based on output from Data Analytics to prioritize a specific region or group of people (to the disadvantage of those left out of these regions or groups) should always be cross-checked and validated by a human being.

6.4 DATA SHARING

Data Analytics Processing may include data sharing with Data Processors or Third Parties, both prior to execution of Data Analytics when the data sets belong to different Data Controllers, and after its completion when results and findings may be shared with Third Parties. It may, therefore, involve both Personal Data and aggregated or anonymized data. Parties with whom data are shared may be new Data Controllers or Data Processors. This data sharing may involve data crossing national borders or being shared by or with International Organizations, depending on the Processing or where the Humanitarian Organization is based. It is important to note that “sharing” includes not only situations where data are actively transferred to Third Parties, but also those when they are made accessible to others. Data sharing involving an international element and a Data Controller/Data Processor relationship are dealt with in more detail below.

6.5 INTERNATIONAL DATA SHARING

Data Analytics routinely involves International Data Sharing of Personal Data with various parties located in different countries. This may involve scenarios such as those listed above, which are summarized below:

- Humanitarian Organizations employing Data Processors, i.e. commercial entities, undertake the actual Processing of Personal Data on the data held by the Humanitarian Organization.
- Humanitarian Organizations asking commercial entities that are and remain the Data Controller of the data to carry out analytics on such data for humanitarian purposes, and provide conclusions/findings to the Humanitarian Organization. Such conclusions could involve either aggregated/anonymized data, or data identifying individuals of possible relevance for Humanitarian Action.
- Sharing data sets among Humanitarian Organizations, public authorities and/or commercial entities (joint Data Controllers and/or Data Processors).
- Actual sharing (or transferring data) to a Humanitarian Organization for Processing by it.

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Data Analytics are conducted, as discussed above.¹⁰³ It is essential to perform a DPIA¹⁰⁴ prior to International Data Sharing for Data Analytics, given the complexity of Data Analytics, the difficulties in ensuring that Data Subjects are adequately informed and are in a position to fully exercise their rights as mentioned above, and the potentially far-reaching implications of Data Analytics for them. Indeed, a DPIA

¹⁰³ See [Section 6.2.2: Legal bases for Personal Data Processing](#).

¹⁰⁴ See [Section 6.7: Data Protection Impact Assessments](#).

will be the most suitable tool to identify the possible risks involved in data sharing, and the most suitable mitigating measures available (e.g. contractual clauses, codes of conduct, or indeed refraining from data sharing).¹⁰⁵

Moreover, when Humanitarian Organizations hire service providers to conduct or support Data Analytics, they should develop an understanding of the purposes for which these companies may use data. Specifically, companies who provide analytics of their own data or who process Humanitarian Organizations' data may have incentives to exploit the findings of the Processing for commercial purposes to improve their understanding of their customers or for further customer profiling. It is therefore very important that any contractual arrangements with them make it completely clear that the purpose of the Processing is and must remain exclusively humanitarian, and that the service provider keeps the humanitarian Processing segregated from its commercial activities. If any doubts arise as to whether the service provider can or will respect this condition, the Humanitarian Organization should refrain from engaging in the Processing. This is because any Processing other than Processing exclusively for Humanitarian Action may have serious implications for Data Subjects. For example, outputs of analytics which identify categories of potential beneficiaries of Humanitarian Action may lead to consequences such as denial of credit, higher insurance premiums, stigmatization, discrimination or even persecution.

Humanitarian Organizations should also be alert to the risk that, in situations of violence or conflict, the parties involved may seek to access and use the findings of Data Analytics to gain an advantage, which would compromise the safety of the Data Subjects and the neutrality of Humanitarian Action. Consequently, in cases where the outputs are potentially sensitive, it is important to consider a scenario where the Humanitarian Organization performs the Data Analytics internally without disclosing the results to the data provider.

6.6 DATA CONTROLLER/ DATA PROCESSOR RELATIONSHIP

The roles of Data Controller and Data Processor are often unclear when conducting Data Analytics. It is thus crucial to determine which parties actually define the purposes and means of data Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers.

¹⁰⁵ See [Chapter 4: International Data Sharing](#) and [Section 4.4: Mitigating the risks to the individual](#).

EXAMPLE 1: Humanitarian Organizations sharing data sets and undertaking Data Analytics using their own organizational resources may be considered joint Data Controllers.

EXAMPLE 2: Humanitarian Organizations sharing data sets but outsourcing the Data Analytics to a commercial service provider that will transfer the findings and keep no records for its own use will be considered joint Data Controllers, and the service provider will be considered a Data Processor.

DPIAs, conducted prior to the Data Analytics operations, may be a suitable means of clarifying the roles of different parties engaged in the Processing.

Once the roles have been clearly defined and the corresponding tasks assigned, it is important to establish which relevant contracts need to be entered into among the data Processing participants. Data collection or International Data Sharing across Humanitarian Organizations and/or national borders and/or third (private or state) bodies should generally be covered by contractual clauses, which can be critical for the following reasons:

- They should clearly allocate the roles between the various parties and, in particular, put them on notice as to whether they are acting as Data Controllers or Data Processors (or both).
- They should contain an outline of the data protection obligations to which each party is subject. This should include the measures that the parties should take to protect Personal Data transferred across borders.
- They should contain obligations to cover data security, responses (objection or notification to the other party) in case of authorities requesting access to data, procedures for handling Data Breaches, Data Processor return/disposal of data at the end of the Processing and staff training.
- They should also require that notice be given to the Humanitarian Organizations involved if any data are accessed without authorization.

6.7 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of applicable data protection regulations and potential risks are covered.¹⁰⁶ DPIAs are now required in many jurisdictions and by some Humanitarian Organizations. However, it can be more difficult to implement them with regard to new technologies, where risks are less clear. Apart from clarifying the details and specifications of the Processing, DPIAs should focus on the risks posed by it and on mitigating measures.

¹⁰⁶ See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

Accordingly, DPIAs need to be conducted prior to any Data Analytics operations. Of particular significance are risk assessment tools that have been specifically developed to assess the risks of Data Analytics in Humanitarian Action, such as the UN Global Pulse Data Innovation Risk Assessment Tool.¹⁰⁷

Indicative risks to be addressed in a Data Analytics DPIA include the following:

- re-identification of individuals of relevance for Humanitarian Action, when the purpose of analytics is to identify patterns
- risks for the viability and security of humanitarian operations, in cases where data of alleged perpetrators of violations of international humanitarian or human rights law are processed
- risks that if a Humanitarian Organization makes requests about specific patterns or categories of individuals of interest to authorities or corporations, this may lead to such Third Parties discriminating or otherwise taking an interest in them with detrimental implications for them and for the neutrality of Humanitarian Action
- risks that the results of the Data Analytics operation performed by Humanitarian Organizations to which a Third Party gains access may be exploited by commercial Third Parties and/or authorities for unrelated purposes
- risk that Data Analytics outputs may be accessed and used by parties in a situation of violence or conflict to gain an advantage vis-à-vis other stakeholders and thus compromise the safety of the Data Subjects and the neutrality of Humanitarian Action
- risk that commercial providers who perform analytics on their own data or who process Humanitarian Organizations' data may have incentives to exploit the findings of the Processing for commercial purposes to improve their understanding of their current or potential customers or for further customer profiling.¹⁰⁸

DPIAs for Data Analytics also take into account the likelihood, magnitude and severity of the harm that could result from the risks. Such risks and harm should then be assessed against the likely expected benefits from Data Analytics and taking into account the principle of proportionality.¹⁰⁹

Specific risk-mitigating measures may include:

- Anonymization as a technical measure
- legal and contractual obligations to prevent possible re-identification of the persons concerned.¹¹⁰

¹⁰⁷ United Nations Development Programme (UNDP), UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*: <http://www.unglobalpulse.org/privacy/tools>.

¹⁰⁸ See [Section 2.3: Aggregate, Pseudonymized and Anonymized data sets](#).

¹⁰⁹ United Nations Development Programme (UNDP), UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*: <http://www.unglobalpulse.org/privacy/tools>.

¹¹⁰ Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*, January 2017, *op. cit.*

DRONES

POSSIBLE USE

SEARCH AND RESCUE
OPERATIONS

MAPPING
EMERGENCY
SITUATIONS

COMPLEMENT
TRADITIONAL
ASSISTANCE

CHALLENGES

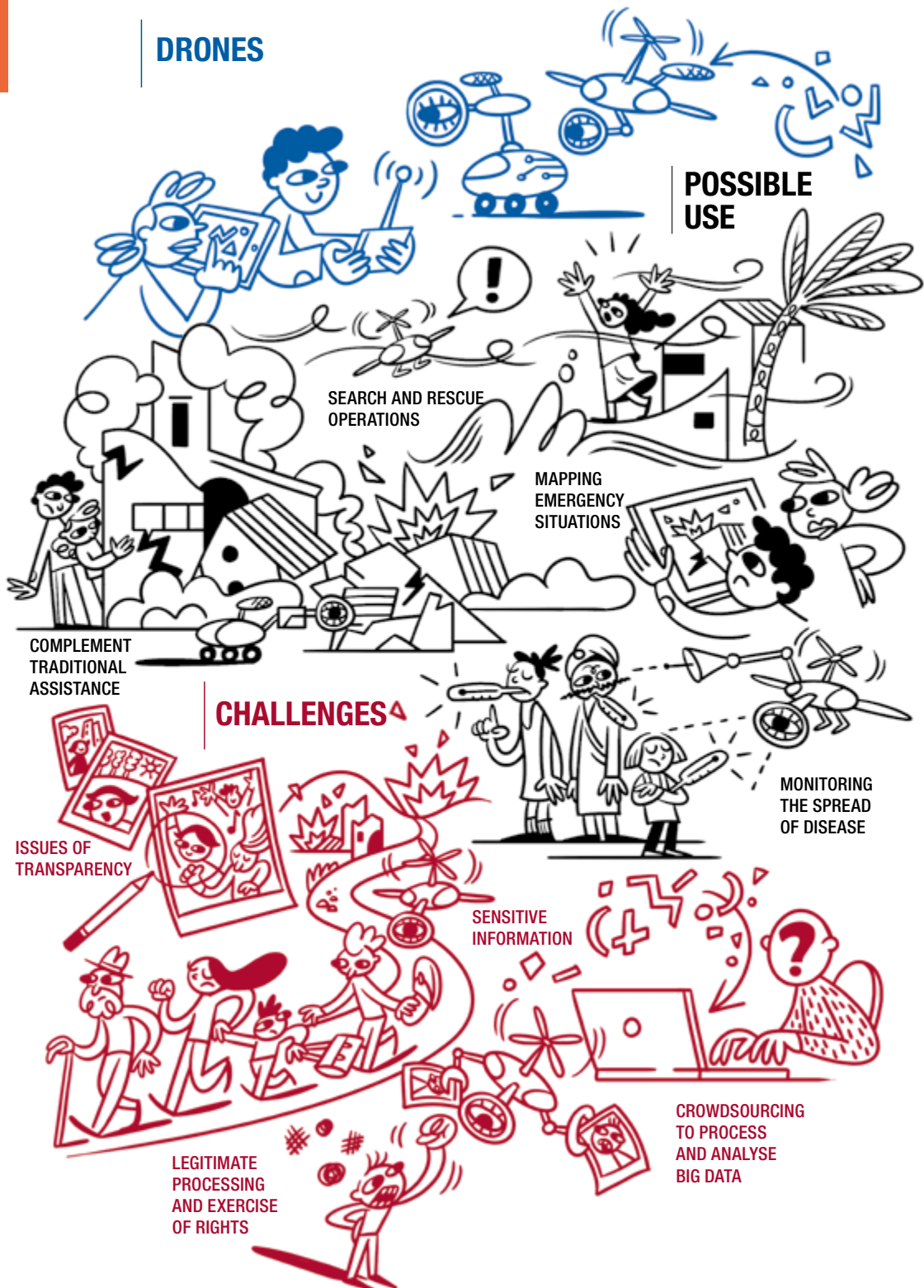
ISSUES OF
TRANSPARENCY

MONITORING
THE SPREAD
OF DISEASE

SENSITIVE
INFORMATION

LEGITIMATE
PROCESSING
AND EXERCISE
OF RIGHTS

CROWDSOURCING
TO PROCESS
AND ANALYSE
BIG DATA



CHAPTER 7

DRONES/UAVS AND REMOTE SENSING

7.1 INTRODUCTION

Drones are a promising and powerful new technology potentially capable of helping Humanitarian Organizations to improve their situational awareness, their response to natural and man-made disasters, and their relief operations. They can complement traditional manned assistance by making operations more efficient, effective, faster and safer. If deployed correctly, Drones could have a significant impact on Humanitarian Action.

Drones are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS). Depending on what they are used for, they are often equipped with cameras, microphones, sensors or GPS devices, all or any of which may make Personal Data Processing possible.

From a data protection perspective various concerns have been raised about the use of Drones. However, it is important to clarify at this early stage that what is of interest in the case of Drones is not their use *per se*, but the different technologies they are equipped with, such as high-resolution cameras and microphones, thermal imaging equipment or devices to intercept wireless communications, because it is these technologies that are used for data collection and Processing. In this respect, the considerations addressed in this chapter could also apply to the use of satellites and, more generally, to remote sensing.

This chapter focuses only on the data protection issues posed by the use of Drones. Other issues and fields of law may be relevant, but will not be dealt with. For instance, guidance will not be provided on air traffic control issues, flight licenses, equipment safety certificates or similar matters.

In general terms, the most common humanitarian use of Drones today entails observation and data collection to enhance situational awareness. Below is an indicative list of the applications for which Drones are or could be used in a humanitarian setting:

- search and rescue
- determining the whereabouts of people unaccounted for
- collection of aerial imagery/situation awareness/post-crisis assessment (e.g. surveying the condition of power lines and infrastructure, assessing the number of wounded people, destroyed homes, dead cattle, etc.)
- monitoring the spread of a disease through the use of heat sensors
- mapping emergency housing settlements
- real-time information and situation monitoring, by providing videos or photos and thus giving an overview
- locating unexploded ordnance (UXO)
- mapping natural disasters or conflict sites

- locating and following people displaced by a Humanitarian Emergency
- delivery of medicines/other rescue equipment in remote areas
- setting up a mesh network/restoring communication networks by relaying signals.

In disaster situations “drones may be used to provide relief workers with better situational awareness, as they can locate survivors amidst the rubble, perform structural analysis of damaged infrastructure, deliver needed supplies and equipment, evacuate casualties, and help extinguish fires – among many other potential applications.”¹¹¹ Drones can also supply aerial data from areas which are considered unsafe for Humanitarian Action providers (e.g. sites contaminated by radioactivity or wildfire locations).¹¹²

Nevertheless, while Drones may be an invaluable source of direct and indirect information when responding to emergencies, a critical assessment has to be made before they are used in any particular case. Their use may include significant risks.¹¹³ Apart from safety issues *per se* (e.g. accidents during their deployment that could result in bodily injury or even death), they may be perceived as spying or intruding in a conflict scenario, something that could severely compromise the safety of their operators and the staff of Humanitarian Organizations, as well jeopardizing local people who may be perceived by the parties in the conflict as having given Consent to the use of Drones on their behalf.

EXAMPLE:

A Humanitarian Organization may have acquired the approval of local community leaders for Drones to be used for the provision of aerial imagery over a large geographical area. However, during its deployment a Drone may accidentally photograph, and consequently provide evidence of, illegal activity taking place in some specific place in the above-mentioned geographical area. The groups carrying out the illegal activity, aware of the drone flying over them, may seek to find and punish the community leaders who provided their approval and also seek the Humanitarian Organizations' operators in order to destroy the evidence collected.

111 Joint Oversight Hearing by the Joint Legislative Committee on Emergency Management and the Senate Committee on Judiciary, *Drones and Emergencies: Are We Putting Public Safety at Risk?*, Background paper, California State Senate, 2015, p. 2: https://sjud.senate.ca.gov/sites/sjud.senate.ca.gov/files/background_paper_-_drones_and_emergencies.pdf.

112 American Red Cross, et. al., *Drones for Disaster Response and Relief Operations*, April 2015, p. 4: <http://www.issue4lab.org/resources/21683/21683.pdf>.

113 Delafoi F, *Le drone, l'allié ambigu des humanitaires*, Le Temps, 11 April 2016: <https://www.letemps.ch/monde/2016/04/11/drone-allie-ambigu-humanitaires>; What do Tanzanians Think About Drones? Now We know, ICT Works, 22 February 2016: <http://www.ictworks.org/2016/02/22/what-do-tanzanians-think-about-drones-now-we-know/>.

As noted above, concerns about potential violations of Personal Data protection rights are not caused by the use of Drones, but rather by the on-board equipment which can process Personal Data. Information technologies embedded in Drones or connected to them can perform various data Processing activities and operations (e.g. data collection, recording, organization, storage and combination of collected data sets). Data typically collected by drones include video recordings, “images (e.g. images of individuals, houses, vehicles, driving license plates, etc.), sound, geolocation data or any other electromagnetic signals related to an identified or identifiable natural person.”¹¹⁴ Depending on the quality of the data, it may be possible to identify individuals directly or indirectly. This can be done either by a human operator or automatically, for instance by capturing an image from a facial recognition programme/algorithm, scanning to detect a smartphone and using it to identify the person or using radio-frequency identification (RFID) chips in passports.¹¹⁵

The following factors may be relevant while assessing Humanitarian Organizations’ data protection response to the use of Drones:

- It is technically possible to make aerial Drones flight-specific, on the basis of unique identifiers embedded in their basic equipment.
- Permission to fly Drones and a remote pilot’s licence issued by the state authorities are required in many countries.¹¹⁶
- Imagery data (of various levels of analysis and quality) are the most common type of data collected by Drones.
- Altitude of flight and angle of capture of the imagery also have a significant impact on the likelihood that the imagery captured may directly or indirectly identify an individual.
- Although technology is advancing rapidly, at present Drones can capture extremely detailed pictures, but most cannot capture individuals’ faces. The picture has to be connected to other data sets in order to lead to identification. When facial identification is not possible, identification may be possible through the use of location and other types of data. The use of metadata (data that provides information about other data) is crucial in this context.
- It is important to establish where data collected are kept and what types of Processing are performed on them; in this respect there is a correlation between Drones and the use of Data Analytics.¹¹⁷
- A number of international initiatives on standards and other drone-use specifications are currently under way, some looking specifically at the use of

114 Article 29 Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, p. 7: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602.

115 *ibid.*, p. 14.

116 Storyhunter Guide to Commercial Drone Regulations Around the World: <https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world>.

117 See [Chapter 6: Data Analytics and Big Data](#).

Drones for humanitarian purposes. Humanitarian Organizations are advised to follow these initiatives closely and apply their findings in their practices.¹¹⁸

- Humanitarian Organizations often outsource the drone operations to professionals, which therefore raises data protection issues (e.g. Data Controller/Data Processor relationship, access to data, etc.).
- Drone-related Personal Data Processing often involves cross-border transfers, which require a legal basis under data protection law.

However, it is worth noting that, given the pace of change in these technologies, a number of the above findings may change substantially in the near future.

Humanitarian Organizations should also realize that, even when identification of individuals is not possible via the use of Drones, their use may still have substantial implications for the life, liberty and dignity of individuals and communities. Humanitarian Organizations should accordingly take precautions to protect Drone-collected data, even if the individuals recorded in them are not immediately identifiable.

EXAMPLE:

If the data from tracking streams of displaced people with Drones are accessed by ill-intentioned Third Parties, vulnerable individuals can be put at risk, even if they cannot be individually identified.

7.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

7.2.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations can process Personal Data collected by Drones using one or more of the following legal bases:¹¹⁹

- the vital interest of the Data Subject or of another person
- the public interest, in particular stemming from an organization's mandate under national or international law
- Consent
- a legitimate interest of the organization
- the performance of a contract
- compliance with a legal obligation.

¹¹⁸ See for example, *Humanitarian UAV Code of Conduct & Guidelines*: <http://uaviators.org/docs>.

¹¹⁹ See [Chapter 3: Legal bases for Personal Data Processing](#).

Lawfully acquiring Consent will most likely prove unrealistic in practice for work carried out by Humanitarian Organizations using Drones.

For example, Consent would not be “freely given” whenever an individual is not free to enter or leave a surveyed area.

This means that Consent as a lawful basis for Personal Data Processing in the context of drone operations by Humanitarian Organizations seems to be generally unrealistic. Drones are used in most cases where there is limited or no access to communities. Even if such access was provided, it would still be almost impossible to obtain Consent from all the people who may potentially be affected by the drone-related Processing. In addition, depending on the circumstances in which Drones might be used, it is questionable whether Consent from people in distress and in need of humanitarian assistance could be considered free.



Courtesy of www.OnyxStar.net

Drones are mostly used where there is limited or no access to people. Even when access is possible, it would still be almost impossible to obtain Consent from all the people who may potentially be affected by drone-related Processing.

The idea of acquiring the “Consent of the community” or the “Consent of authorities” has also been suggested for the use of Drones in Humanitarian Action as a plausible alternative to individual Consent. This could involve, for example, obtaining Consent only from representatives of a group of vulnerable individuals and not the individuals themselves. However, under data protection law Consent must be provided by the individual.

EXAMPLE:

Community leaders or the state authorities concerned could give their Consent to the use of Drones by a Humanitarian Organization in order to map a refugee camp, but the individuals present in the area may not be aware of the Drones, or not wish to be photographed/have their Personal Data collected by Drones.

Where Consent cannot be obtained from the individual concerned, Personal Data can still be processed by the Humanitarian Organization if it establishes that this may be in the vital interest of the Data Subject or of another person, or if another legal basis applies (as noted in 7.2.1). In other words, Personal Data can be processed where the Processing is necessary in order to protect an interest which is essential for the Data Subject’s life, integrity, health, dignity, or security or that of another person.

As has already been mentioned in [Chapter 3: Legal bases for Personal Data Processing](#), given the nature of Humanitarian Organizations’ work and the emergency situations in which they operate, in some circumstances there may be a presumption that the Processing of data necessary for humanitarian purposes is in the vital interest of a Data Subject.¹²⁰

The use of Drones by Humanitarian Organizations should be assessed in each particular case to determine whether it is actually necessary for the protection of the vital interests of the Data Subject or another person. The Drones’ contribution to the protection of overriding private interests such as life, integrity and security has to be proven or, at least, be probable given the type and scale of the emergency, or concerns about a lack of information relating to the emergency, which could only be remedied by the use of Drones. Strict standards should therefore be applied to determine whether this legal basis is present.

¹²⁰ See EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, *op. cit.*, Recital 46.

EXAMPLES:

The use of Drones in search and rescue operations by a Humanitarian Organization would most likely qualify under this legal basis, because it would protect the vital interest of the Data Subject (i.e. the person unaccounted for).

The use of Drones in mapping operations by a Humanitarian Organization, in the absence of a specific emergency, would most likely not qualify under this legal basis, because there is no direct connection with the vital interests of the Data Subjects living or moving around in the areas being mapped.

It is important for Humanitarian Organizations to make careful assessments when important grounds of public interest are triggered and are to be used as a lawful basis for Processing Personal Data collected by Drones. For example, this will usually be the case when the activity in question is an important part of a humanitarian mandate established under national or international law (e.g. for the ICRC, IFRC, National Red Cross and Red Crescent Societies, UNHCR, UNICEF, WFP or IOM).

Humanitarian Organizations may also process Personal Data collected by Drones where this is in their legitimate interest, and provided that this interest is not overridden by the Data Subjects' fundamental rights and freedoms. A legitimate interest of an organization can be established when Personal Data Processing is necessary to further or support its mission. It can be argued, however, that where no public or vital interest can be established, it may be difficult to envision circumstances in which the rights and freedoms of the Data Subjects would not override the organization's legitimate interest, particularly in cases where the individuals whose Personal Data are likely to be captured cannot be informed, nor can they effectively exercise their data protection rights.

EXAMPLE:

A Humanitarian Organization may use a Drone to demonstrate successful completion of an action, for instance, to collect footage for a promotional video. This may fall under the legal basis of legitimate interest, although careful consideration of the potential infringement of the rights and freedoms of the individuals appearing in the video would need to be undertaken. In this respect, the extent to which Data Subjects can be informed and effectively exercise their rights (including the right to object) are critical factors.

7.2.2 TRANSPARENCY/INFORMATION

The principle of transparency requires that at least a minimum amount of information concerning the Processing be provided to the Data Subject. In addition, information and communications about the Processing should be easily accessible and easy to understand, express in clear and plain language. For obvious practical reasons these requirements can be difficult to satisfy in the case of Drones. Timing of information is also important; in non-emergency situations, this should ideally take place in advance of and during Drone flights. The involvement of community leaders and authorities or media campaigns targeted at the envisaged Data Subjects (e.g. radio, newspapers and posters in public areas) can help fulfil transparency obligations.

EXAMPLE:

In order to fulfil transparency and information obligations, Humanitarian Organizations using Drones could affix their marks and signs on them; maintain websites or provide relevant information on social media; use available local communication channels (e.g. radio, television, the press); and hold discussions with community leaders.

7.2.3 PURPOSE LIMITATION AND FURTHER PROCESSING

The specific purpose/s for which Personal Data are collected should be explicit and legitimate. Humanitarian Organizations may use Drones for purposes such as the following:

- search and rescue
- determining the whereabouts of people unaccounted for
- collection of aerial imagery, situation awareness, post-crisis assessment (e.g. locating displaced people who need help, surveying the condition of power lines and infrastructure, assessing the number of wounded persons, destroyed homes, dead cattle, etc.)
- monitoring the spread of a disease through the use of heat sensors
- crowd modelling in protests
- mapping emergency housing settlements
- real-time information and situation monitoring, by providing videos or photos and thus giving an overview
- mapping of natural disasters or conflict sites
- locating unexploded ordnance (UXO)
- locating and following people displaced by a Humanitarian Emergency
- delivery of medicines, other rescue equipment in remote areas
- setting up a mesh network or restoring communication networks by relaying signals.

It was also established in [Chapter 2: Basic principles of data protection](#) that, irrespective of the legal basis used for the Processing, Humanitarian Organizations may process Personal Data for purposes other than those specified at the time of collection where such Further Processing is compatible with those initial purposes.

7.2.4 DATA MINIMIZATION

Personal Data may only be processed if adequate, relevant and not excessive in relation to the purposes for which they were collected. Therefore, a strict assessment of the necessity and proportionality of the processed data should take place.¹²¹ Moreover, when Drones are used for humanitarian purposes, the principle of data minimization should be respected by choosing proportionate technology and by adopting measures of data protection and privacy by design and by default.

For instance, Humanitarian Organizations could consider the following options:

- Privacy settings on services and products should by default avoid the collection and/or the Further Processing of unnecessary Personal Data.
- Anonymization techniques should be implemented.
- Faces/human beings should be blurred automatically (or only certain particular categories of more vulnerable individuals).
- Flight altitude or angle of capture of imagery should be increased to minimize the likelihood of capturing imagery that can directly identify individuals.

7.2.5 DATA RETENTION

Personal Data processed via Drones should not be stored for a period longer than necessary for the purpose of the Processing. In other words, collected data should be deleted or anonymized when the purpose for which they were collected has been served. The adoption of storage and deletion schedules is also advisable. Data collection devices, carried by Drones or connected to them remotely, should be designed in such a way that, should they need to retain data, a defined storage period for the Personal Data collected can be set and, as a result, Personal Data which are no longer necessary can be automatically deleted according to defined schedules.

EXAMPLE:

Data collected by Drones to help a Humanitarian Organization respond to an incident should, in principle, be deleted when the incident has been dealt with successfully; if the Humanitarian Organization wishes to archive this information (for instance, for historical purposes), it should take adequate measures to protect the integrity and security of the data and to prevent any unauthorized access.

¹²¹ See [Chapter 2: Basic principles of data protection](#).

7.2.6 DATA SECURITY

A Humanitarian Organization deploying Drones should implement adequate security measures that are appropriate for the risks involved.¹²² For Drones, this could include encryption of databases or temporary storage devices on board, as well as end-to-end encryption of data in transit between the drone and the base, where applicable.

7.3 RIGHTS OF DATA SUBJECTS

The rights of the Data Subject have already been described in [Chapter 2: Basic principles of data protection](#). The following are some further remarks about Data Subjects' rights with respect to Humanitarian Organizations' use of Drones.¹²³

As far as the right to information is concerned, Data Subjects exposed to Drone-related Processing should be provided with the following:

- the identity of the Data Controller of the Drone and of its representative
- the purposes of the Processing
- the categories of Personal Data collected
- recipients or categories of recipients of the data
- the existence of the right of access to and the right to specify and correct the data concerning them
- the existence of the right to object, where this is realistic.

In practice, however, it could prove challenging for Humanitarian Organizations to provide Data Subjects with information along the above lines when using Drones to collect Personal Data. Nonetheless, the various options to be decided on a case by case basis could include: information campaigns, public notices and other similar measures. Drone operators should publish information on their website or on dedicated platforms to inform individuals about the different operations that have taken place as well as forthcoming ones. In remote areas or where it is unlikely that individuals can access the internet, information can be published in newspapers, leaflets or posters, or provided by means of a letter or radio broadcast.

As far as drone applications that may cover larger geographical areas are concerned, where the provision of information to Data Subjects proves difficult or impossible, the creation of a national or cross-national information resource (easier to trace than websites of single operators) has been suggested to enable individuals to identify the missions and operators associated with particular Drones.

¹²² See [Chapter 2: Basic principles of data protection](#).

¹²³ See [Section 2.11: Rights of Data Subjects](#).

Data subjects should also have the right to opt out of the Processing, even though this can be challenging in the case of Drones, as individuals might not be able to avoid the surveyed area. Furthermore, Humanitarian Organizations are strongly encouraged to implement complaint procedures in their Personal Data Processing practices and internal data protection policies. These procedures should enable data correction and erasure. However, it should be recognized that there may be legal bases for data Processing that do not allow the exercise of all individual rights (for instance, requests for opt-outs by individuals may not be observed in the event of Processing undertaken under the public interest legal basis described above).

Finally, as far as the right to access information is concerned, access should be limited in order to mitigate the risks that access by one Data Subject could expose the Personal Data of other Data Subjects, or that ill-intentioned Data Subjects may take action detrimental to vulnerable individuals, whether identifiable or not.

Limiting access exclusively to aerial imagery or footage including Personal Data of a Data Subject is particularly challenging, since, by its nature, it may include Personal Data of many other individuals and it is highly unlikely that it may be practicably and meaningfully redacted.

EXAMPLE:

In the case of aerial photography collected by Drones, the exercise of the right to access by Data Subjects may require the blurring of other faces or Personal Data not related to the applicant; in the same cases, the right to object could include de-identification of the applicant's Personal Data on the same photograph, but not the destruction of the photograph itself or the Personal Data of other individuals appearing on it.

7.4 DATA SHARING

The circumstances under which personal information is exchanged between Humanitarian Organizations or between Humanitarian Organizations and Third Parties need to be identified and addressed with respect to data protection. Information collected by Drones may be shared either at the moment of collection or at a later stage. Humanitarian Organizations may outsource drone-related work to Data Processors. In the event that any of the above involves Personal Data being shared across national borders, the relevant issues concerning International Data Sharing also need to be addressed.¹²⁴

In these cases, it is important to consider:

¹²⁴ See [Chapter 4: International Data Sharing](#).

- the data protection roles of the Humanitarian Organizations concerned¹²⁵
- whether imagery or other information exchanged should include Personal Data or whether it is sufficient to share only the conclusions and findings of the analysis and assessment of the imagery collected (no raw data exchange)
- involuntary or accidental data sharing (e.g. if imagery is saved on the device and the device is captured), or if an aerial imagery feed is transmitted in a non-secure and unencrypted way; the impact of this should also be taken into consideration by the Humanitarian Organizations involved.

Crowdsourcing is a common way of Processing and analysing large data sets collected by Drones. Its importance derives from the fact that aerial imagery or footage is often massive and reviewing all this material is impossible for Humanitarian Organizations themselves. An increasingly common practice is to post the imagery online and invite volunteers to review it in order to spot, for instance, interrupted power lines, destroyed houses, affected people, and cattle, etc. However, this can have severe negative consequences (e.g. enabling access to online material by potentially ill-intentioned Third Parties). It is important, therefore, to ensure that:

- the volunteers accessing the imagery are vetted and trained by the Humanitarian Organization
- the volunteers commit to a Processing agreement which includes provisions covering discretion and confidentiality
- the material is not published or otherwise shared beyond the group of vetted volunteers
- volunteers receive appropriate support to understand the purpose of the data Processing
- volunteers' Processing is properly logged.

7.5 INTERNATIONAL DATA SHARING

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Drones are used, as discussed in [Chapter 4: International Data Sharing](#). Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and in line with their own internal policies before carrying it out. Performing a DPIA prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing.¹²⁶

¹²⁵ See [Section 7.6: Data Controller/Data Processor relationship](#).

¹²⁶ See [Section 7.7: Data Protection Impact Assessments](#).

7.6 DATA CONTROLLER/ DATA PROCESSOR RELATIONSHIP

The roles of Data Controller and Data Processor may be unclear when operating Drones or when Processing data collected by them. As noted, outsourcing is also frequent in drone-related Processing. It is thus crucial to determine which parties actually determine the purposes and means of data Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers.

EXAMPLES:

A Humanitarian Organization whose own staff operate Drones for its own purposes is the (only) Data Controller for such Processing.

A Humanitarian Organization outsourcing a Drone operation to a specialized corporation, whose sole task is to pilot the Drones, would be the (only) Data Controller for such Processing; the corporation would be the Data Processor for this operation.

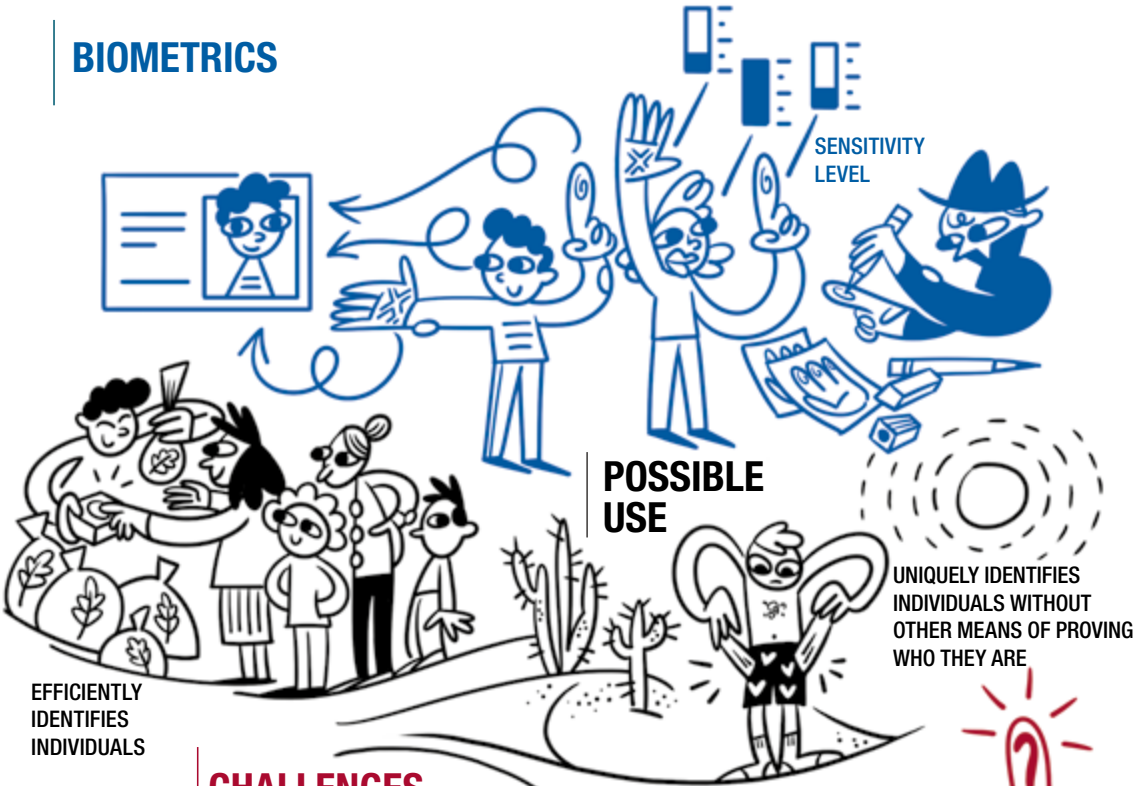
Two Humanitarian Organizations who wish to use Drones and outsource all relevant operational work to a corporation having no access to the data collected will be joint Data Controllers. The corporation would be the Data Processor for the operation.

7.7 DATA PROTECTION IMPACT ASSESSMENTS

As discussed in [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#), DPIAs are important tools used during project design to ensure that all aspects of data protection regulations and applicable risks are addressed. Apart from clarifying the Processing details and specifications, DPIAs should focus on the risks posed by the operation as well as on mitigating measures. In this regard, it is important to note that DPIAs should be drafted prior to any Drone operations.

In order to avoid hindering humanitarian operations, template DPIAs for the use of Drones should be developed beforehand. These templates should cover the specific risks and considerations outlined in the present chapter and be easy and quick to complete and implement.

BIOMETRICS



EFFICIENTLY
IDENTIFIES
INDIVIDUALS

POSSIBLE
USE

UNIQUELY IDENTIFIES
INDIVIDUALS WITHOUT
OTHER MEANS OF PROVING
WHO THEY ARE

CHALLENGES



RELIABILITY
OF DATA

DATA
MINIMIZATION

TECHNICAL
DIFFICULTIES

IRREVERSIBLE

DIFFICULTIES
WITH CONSENT

HUMANITARIAN PURPOSE
ETHICAL ISSUES

CHAPTER 8

BIOMETRICS

8.1 INTRODUCTION

The International Organization for Standardization defines biometric recognition and Biometrics as the “automated recognition of individuals based on their biological and behavioural characteristics”.¹²⁷ Biometrics are therefore measurable, unique human signatures that may include fingerprints, iris scans or behavioural characteristics such as the way a person walks.

The data protection implications of the use of biometric data, with particular reference to the use of biometric data in passports, identity cards and travel documents, have been highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Biometrics, adopted in Montreux, Switzerland, in 2005.¹²⁸

Humanitarian Organizations around the world increasingly deploy biometric recognition as part of their identification systems because of the benefits it can bring in efficiently identifying individuals and preventing fraud and/or misuse of humanitarian aid. Indeed, paper-based identification mechanisms (identity cards, ration cards, wrist bands, etc.) that constitute the non-digital alternative have limitations, as they may easily be lost or counterfeited, require substantial resources to crosscheck (thereby giving rise to potential duplication and inefficiency), and in most cases do not allow for automated Processing. In certain situations, it is suggested that these shortcomings may be overcome through the use of biometric identification systems (often as an additional means of verification). Biometric data are more difficult to counterfeit and, being digitally produced and stored, facilitate the efficient management of humanitarian aid in the field and can also be used for Data Analytics or other types of advanced data Processing operations. In addition, by focusing on the individual’s unique features, Biometrics can confirm the identity of individuals who have no other means of adequately proving it, which is often the case with displaced people, and therefore put individual identity and dignity at the heart of Humanitarian Action.¹²⁹

¹²⁷ See ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics: <https://www.iso.org/standard/66693.html>.

¹²⁸ International Conference of Data Protection and Privacy Commissioners, Resolution on Use of Biometrics in passports, identity cards and travel documents, Montreux, Switzerland, 2005: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Biometrics-in-passports-identity-cards-and-travel-documents.pdf?mc_phishing_protection_id=28047-br1tehqu81eaoar3q10.

¹²⁹ See for example, Hugo Slim, *Eye Scan Therefore I am: The Individualization of Humanitarian Aid*, European University Institute Blog, 2015: <https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/>; Paul Currión, *Eyes Wide Shut: The challenge of humanitarian biometrics*, IRIN, 2015: <http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics>.

However, these promises have not always been fulfilled in the actual deployment of Biometrics identification systems. Some projects to implement Biometrics have reportedly faced considerable problems with regard to the reliability of the relevant systems.¹³⁰ Inherent limitations, such as the fact that individuals' fingerprints are not always readable, provide further difficulties in implementation. Ethical issues may also arise, for example, by virtue of the use of biometric data in national identification systems and the problematic legacies of such systems in certain countries.¹³¹ Additionally, due to the interest in biometric data for national law enforcement and national security purposes, Humanitarian Organizations may find themselves under increasing pressure to share data with national and regional authorities for purposes which go beyond humanitarian work. Interest in biometric data means that it faces a significant risk of unauthorized access by Third Parties i.e. hacking.

Humanitarian Organizations may use biometric technologies for Processing operations such as the collection and management of data on displaced persons who have to be registered for the purposes of humanitarian aid distribution, including aid delivered through cash and vouchers.¹³²

For the time being, technologies used for the above Processing operations involve mainly automatic fingerprint recognition systems (fingerprints being the dominant form of biometric data collected) and iris scans. Other forms of biometric data could, however, be envisaged, including:

- palm vein recognition
- voice recognition
- facial recognition
- behavioural characteristics.

The benefits of the use of biometric technologies by Humanitarian Organizations could include:

- accurate individual identification
- combating fraud and corruption
- increased donor support and credibility of programming (as a consequence of the points above)
- greater efficiency through the digital Processing of identification data
- greater efficiency in the physical protection of individuals/minimization of the risk of disappearance
- putting individual identity and dignity at the heart of Humanitarian Action

130 Gus Hosein and Carly Nyst, *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, IDRC/UKaid, 2014, p. 16.

131 *Ibid.*, p. 19.

132 See [Chapter 9: Cash transfer programming](#).

- enhancing the right of individuals to move freely
- enhancing the resettlement of individuals into third countries
- enabling bank account acquisition.

However, a number of risks and challenges have equally been raised:

- reliability and accuracy of data (including the risk of false matches) and/or of systems – the quality of the biometric identification system ultimately depends upon the quality of the sensors used and the quality of the Biometrics provided
- inherent technical difficulties (e.g. the unreadability of fingerprints in the case of certain beneficiaries with depleted fingerprints)
- biometric information is unique and cannot be modified
- ethical issues (cultural sensitivities, beneficiaries' perceptions and/or concerns about surveillance)
- function creep (same systems used for other purposes than the ones originally designated, including non-humanitarian purposes)
- possible pressure by various national or regional authorities (including donors) to acquire the biometric data sets collected by Humanitarian Organizations, with the risk of the data being used for purposes other than strictly humanitarian purposes (e.g. law enforcement, security, border control or monitoring migration flows).

It is very important, therefore, that Humanitarian Organizations carefully analyse and consider the possible need for the use of biometric data, and clearly and transparently set out how they intend to use them in a way that is compatible with Data Protection requirements, ideally through public policies on the use of biometric data.¹³³

8.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The use of biometric technologies raises significant data protection issues. Biometric information is considered to be Personal Data and therefore covered by data protection legislation. For example, the EU General Data Protection Regulation expressly regulates biometric data, defining them as “Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.”¹³⁴ In many

¹³³ See for example the Policy on the Processing of Biometric Data by the ICRC, <https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/>.

¹³⁴ EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, *op. cit.* Article 4(14).

legal systems, biometric information is considered to be “Sensitive Data.”¹³⁵ Consequently, special, detailed requirements apply to the Processing of this type of data, directly affecting the lawfulness of the Processing in the event that they are not met.

This higher level of protection is justified due to the following special characteristics of biometric information:

- it is unique and cannot be modified, consequently increasing the risks involved in identity theft; and
- technological developments may affect its Processing in unpredictable ways, because the type of personal biometric data collected today may reveal a great deal more information about an individual in the future (e.g. retina information revealing genetic information, ethnic origin, health conditions and age).

Accordingly, while a basic assumption underlying this Handbook is that it is not possible in Humanitarian Action to establish clear-cut categories of Personal Data requiring special protection (because data that may not be sensitive in one emergency situation may be sensitive in another and vice versa), there is an assumption that biometric data require special protection, irrespective of the situation and the circumstances. It is for this reason that DPIAs should always be carried out before Biometrics are used.

When undertaking DPIAs, Humanitarian Organizations should take into account the fact that different types of biometric data may have different levels of “sensitivity”. Some categories of biometric data, while sensitive for the reasons set out above, may be more or less sensitive than others. Fingerprints, for example, may be depleted or erased, whether unintentionally (e.g. through heavy manual work), or intentionally, thus making this type of data less sensitive than others. On the other hand, iris scans may potentially enable the extraction of very sensitive information beyond the identification of the individual. Furthermore, certain types of biometric data may only be collected and read with the direct participation of a Data Subject, such as palm vein recognition, thus making this type of data less sensitive than others. Other categories of biometric data, such as iris information, can be read from a distance, thus making it particularly sensitive.¹³⁶

Consequently, even when the legislation governing Personal Data Processing mentioned above does not apply, Processing biometric data presents special risks and requires an increased level of care. Processing should therefore be subject to

¹³⁵ For example, in the EU biometric data are considered to be a special category of Personal Data: EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, *op. cit.* Article 9.

¹³⁶ See for example: *How Facial Recognition Might Stop the Next Brussels*, 22 March 2016, <http://www.defenseone.com/technology/2016/03/how-facial-recognition-might-stop-next-brussels/126883/>.

a careful preliminary review, in order to establish whether certain safeguards (for example, increased security measures) need to be in place before, during and after its execution, as discussed further below, or if biometric data should be used at all, considering the potential risks involved.

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

8.2.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data using one or more of the following legal bases:¹³⁷

- the vital interest of the Data Subject or of another person
- the public interest
- Consent
- a legitimate interest of the Organization
- the performance of a contract
- compliance with a legal obligation.

As discussed in [Chapter 3: Legal bases for Personal Data Processing](#), while Consent is the preferred legal basis for Personal Data Processing to take place, it may be difficult to prove validity of Consent in a humanitarian situation. However, biometric data are considered to be Sensitive Data, and therefore, Data Controllers should obtain individuals' Consent. In addition, given that biometric information may only be collected directly from the individuals concerned, and in contrast with some other methods of data collection and Processing, it is generally feasible for Humanitarian Organizations to obtain Consent to use biometric data. However, it will not always be possible for Humanitarian Organizations to collect unambiguous, free, informed and documented Consent for the Processing of biometric data, for reasons also set out in [Chapter 3: Legal bases for Personal Data Processing](#), such as:

- the individuals' physical inability to provide it, such as in cases of unconscious patients (where, for example, biometric data may be required to unlock a patient medical file, combined with other legitimate authority to unlock)
- the shortage of time and staff to ensure adequate counselling during the first phases of an emergency, when the priority is to provide lifesaving assistance
- the individuals' vulnerability and/or legal inability to provide it
- the highly technical nature and irreversible nature of the data potentially exposing individuals to risks that are difficult to understand or contemplate when Consent is given. This refers particularly to the possibility that science and technology may develop in ways that pose new risks not foreseen at the time of Consent (e.g. genetic information becoming accessible from a scan of an individual's iris)

¹³⁷ See [Chapter 3: Legal bases for Personal Data Processing](#).



A Syrian refugee scans her iris at a branch of the Cairo Amman Bank to access monthly cash assistance, Amman, Jordan.

- no real choice is provided as to alternative ways of receiving assistance or protection (for example, if you are dependent on humanitarian aid for your survival or that of your family, or if you need to register to remain legally in the country in which you are located, there is very limited opportunity for you to refuse the collection of your biometric data).

When valid Consent cannot be obtained from the individual, i.e. the Data Subject, Personal Data can still be processed by the Humanitarian Organization concerned if it establishes that this is necessary for reasons of substantial public interest or that it is in the vital interest of the Data Subject or of another person, i.e. where data Processing is necessary in order to protect an interest which is essential for the Data Subject's life, integrity, health, dignity, or security, or that of another person.

In some cases, the nature of Humanitarian Organizations' work and the emergency conditions in which they operate in armed conflicts and other situations of violence lead to a presumption that their Processing of Personal Data is in the vital interest of a Data Subject or another person (for instance, in cases of imminent threats against the physical and mental integrity of the persons concerned).

It could be argued that in difficult conditions, because of the effectiveness of Biometrics to identify individuals, the vital interests of the Data Subject or another person might constitute a plausible alternative legal basis for the relevant Processing in cases when Humanitarian Organizations are unable to obtain the

individuals' Consent. Furthermore, it is possible to imagine a situation in which the use of biometric systems can be argued to be justified by the promotion of the beneficiaries' vital interests. For example, if only limited resources are available for Humanitarian Action and some potential beneficiaries do not receive essential assistance because aid is fraudulently overprovisioned to another group of individuals, biometric systems can facilitate accurate resource allocation and fraud prevention. On the other hand, it can also be argued that biometric data are not essential for the purposes of distributing aid. The use of biometric data responds more to the Humanitarian Organizations' need to carry out their work in an efficient and effective manner, avoiding the risk of duplication and the waste of financial resources, rather than responding to the vital interests of the individuals concerned.

In addition, it is important to clarify the life cycle of biometric data. If these data are intended to be used for the entire duration of an individual's life, then the legal basis of that person's vital interest will most likely not be applicable, and Consent should be acquired instead.

A final consideration in this area relates to the intrinsic value of biometric data in enabling the establishment of a clear, univocal, identity to persons affected by Humanitarian Emergencies and the role that this could have in restoring and/or strengthening the dignity of the individual, including allowing the individual to exercise their rights. In this light, the vital interests of the individual as Data Subject may indeed be at stake.

In some cases, important grounds of public interest may be used as the legal basis for Processing biometric data. For example, this will usually be the case when the activity in question is part of a humanitarian mandate established in national or international law. Cases where this may be relevant include distributions of assistance, where it may not be possible to obtain the Consent of the beneficiaries. It is important to note that if the life, security, dignity and integrity of the Data Subject or of other people are at stake, then vital Interest may be the most appropriate legal basis.

Public interest could constitute the suitable legal basis for Processing biometric data where a mandate to carry out Humanitarian Action is established in national, regional, or international law, and where Consent and or vital interest do not apply, as per the cases discussed above.

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. Such legitimate interests may include Processing necessary to increase the efficiency of the delivery of humanitarian assistance, reduce costs and risks of duplication and fraud. However, considering that biometric data can be used for potentially intrusive purposes and given their

specific features highlighted above, it can be questioned whether the rights and freedoms of a Data Subject do not always override the legitimate interests set out above. Before the legitimate interests of the Data Controller can be used as a legal basis, a careful analysis of the risks and of possible interference with the fundamental rights and freedoms of the Data Subject would have to be included in the relevant DPIA. This is particularly important in cases where a risk may be envisaged that Third Parties could gain unauthorized access to the data, or put pressure on Humanitarian Organizations to provide this highly Sensitive Data and use them for other than exclusively humanitarian purposes.

8.2.2 FAIR AND LAWFUL PROCESSING

Under data protection law, Personal Data need to be processed lawfully and fairly.¹³⁸ Lawfulness of the Processing refers to the identification of an appropriate legal basis. The requirement for fairness is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations involved in biometric data Processing should keep in mind that these principles need to be applied during all stages of Processing.

8.2.3 PURPOSE LIMITATION AND FURTHER PROCESSING

As discussed in [Chapter 2: Basic principles of data protection](#), at the time of collecting Personal Data the Humanitarian Organization concerned should determine and set out the specific purpose/s for which data are processed. The specific purpose/s should be explicit and legitimate and could include humanitarian purposes such as distributing humanitarian assistance, restoring family links, protecting individuals in detention, providing medical assistance, or forensic activities.

The purposes of the Processing need to be clearly communicated to individuals at the time of collection. Given that biometric information is used for individual identification, the purposes of the Processing should refer to the initial purposes of the identification (e.g. identification itself, aid disbursement whether through in-kind items or cash payments).

Personal Data may be processed for purposes other than those initially specified at the time of collection where the Further Processing is compatible with those purposes, including where the Processing is necessary for historical, statistical or scientific purposes. In order to establish whether Further Processing is compatible with the purpose for which the data were initially collected, attention should be paid to the following factors:

- any link between the purposes for which the data were collected and the purposes of the intended Further Processing

¹³⁸ See [Section 2.5.1: The principle of the fairness and lawfulness of Processing](#) and [Section 8.2.2: Fair and lawful Processing](#).

- to what extent the Further Processing is humanitarian in nature
- the situation in which the Personal Data were collected, in particular regarding the relationship between Data Subjects and the Data Controller
- the nature of the Personal Data
- the possible consequences or risks of the intended Further Processing for Data Subjects
- the existence of appropriate safeguards
- the reasonable expectation of the Data Subjects as to possible further uses of the data.

EXAMPLE:

If a Biometrics identification system is deployed for aid distribution by a Humanitarian Organization, and the individuals concerned have consented to this, the same system cannot be used to transmit participants' data to donors of the Humanitarian Organization for cross-referencing purposes, unless the participants also consented to this purpose.

In considering the above factors, the humanitarian aspects of the Processing purpose should be given particular consideration.

As explained above,¹³⁹ purposes within the wider category of “humanitarian purposes” are likely to be compatible with Further Processing operations. This would, however, not be the case if new risks are involved, or if the risks for the individuals concerned outweigh the benefits of Further Processing. This assessment would depend on the circumstances of the case, and include an analysis of any risks that Processing may be against significant interests of the person to whom the information relates or his/her family, in particular, when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or reputation.

In the same vein, Further Processing for non-humanitarian purposes (e.g. for law enforcement or national security, security checks, migration flux management or asylum claims) should be deemed to be incompatible with the initial Processing undertaken by the Humanitarian Organization. Similarly, purposes which could be interpreted as humanitarian purposes, but involving new risks for the individuals, such as migration management and asylum claims, or identification by authorities, cannot be deemed to constitute compatible Further Processing.

¹³⁹ See [Section 8.2.3: Purpose limitation and Further Processing](#).

8.2.4 DATA MINIMIZATION

The Personal Data processed should be adequate and relevant for the purposes for which they are collected. In particular, this means ensuring that the data collected are not excessive and that the time period for which the data are stored is limited to the minimum necessary. The amount of Personal Data collected and processed should, ideally, be limited to what is necessary to fulfil the specified purpose of data collection and data Processing or compatible Further Processing.

Biometric information collected for identification purposes needs to be proportionate to these purposes. This means that only the amount of biometric information necessary for the identification of individuals needs to be collected and processed; any “excess” information that is not relevant to the identification should not be collected and, if collected, should be deleted. Similarly, the range of biometric data sets collected should be limited to what is proportionate (e.g. collecting facial imagery or iris scans may not be considered as proportionate if photos and fingerprints are already being used for identification purposes).

Compartmentalization of data collected within a Biometrics system (i.e. with access being provided on a need-to-know basis) could provide a meaningful way for Humanitarian Organizations to address data minimization requirements.

Also, when designing a programme involving biometric data collection, the data minimization principle should guide Humanitarian Organizations to collect as few biometric identifiers as possible in order to achieve the purpose of identification for the specific Humanitarian Action.

EXAMPLE:

For the purposes of identifying a beneficiary and avoiding fraud and duplication, collection of one source of biometric data may be sufficient (such as one fingerprint), and collection of a combination of more than one fingerprint and iris may be disproportionate and in breach of the data minimization principle.

8.2.5 DATA RETENTION

Biometric information poses security challenges that may be addressed through either deletion or destruction after completion of their Processing or a carefully structured data retention policy, which would describe the conditions for deletion or destruction or other options to be applied, such as de-identification or access restriction. Retention for Further Processing, therefore, should be avoided, unless such Further Processing is clearly defined and required within the necessary retention period for the purposes for which the data were originally collected. Humanitarian Organizations need to develop their own internal data retention policies, based on the type of data collected and their potential uses in the future.

8.2.6 DATA SECURITY

Given the sensitive nature of biometric information as well as its potential misuse if unauthorized access is granted to it or otherwise obtained,¹⁴⁰ it is imperative that adequate, proportionate security measures are implemented by the Humanitarian Organization determining the purposes and means of the Processing (i.e. by the Data Controller). For example, encryption or compartmentalization of information could constitute viable solutions to this end for Humanitarian Organizations.

8.3 RIGHTS OF DATA SUBJECTS

The rights of the Data Subject as described in [Chapter 2: Basic principles of data protection](#) include the rights to information, access, correction, deletion and objection.

With regard to the right to information, when data are collected directly from the individuals concerned, such as in the case of biometric data, it is often easier for Data Controllers to provide them with adequate information as to the details of Processing. The level of information to be provided if data are processed on the basis of Consent will be high, considering the significant additional risks involved. This should include information as to the possible implications of biometric data being accessed by Third Parties as part of the Processing required to implement the Biometrics project. Additional access by Third Parties may not be contemplated initially, nor the possible consequences known. This may be the case, for example, when sharing with resettlement states for resettlement Processing. This scenario, not anticipated at the time of collection, would require a separate Consent collection after initial registration/biometric enrolment.

Adequate infrastructure should be put in place to facilitate the rights to access, objection, deletion and rectification when Biometrics are used. In this regard, it is advisable to define complaint procedures in internal data protection policies and implement them in Personal Data Processing practices.

8.4 DATA SHARING

Biometrics Processing may include data sharing with Third Parties in the following scenarios:

- The Humanitarian Organization hires an external Data Processor to provide the Biometrics technology required to collect and process the data. In this case a Data Controller/Data Processor relationship is established.

¹⁴⁰ Sarah Soliman, *Tracking Refugees With Biometrics: More Questions Than Answers*, War on the Rocks Blog, 9 March 2016: <https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questions-than-answers/>.

- The Humanitarian Organization carries out a transfer of data to a Third Party, which becomes a new Data Controller.
- The authorities of the host country request or require a copy of biometric data collected on their territory, either in bulk or for specific individuals.

It is important to take into consideration data protection requirements before undertaking such sharing, and to note that “sharing” includes not only situations where data are actively transferred to Third Parties, but also those when they are made accessible to others. Because of the sensitivity of Biometrics data, particular caution should be used before any data sharing is carried out.

8.5 INTERNATIONAL DATA SHARING

Biometric information Processing may involve the sharing of Personal Data with various parties located in different countries, such as in the case of International Data Sharing among different Humanitarian Organizations, or International Data Sharing among Humanitarian Organizations and private or public sector Third Parties.

Data protection law restricts International Data Sharing and Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Biometrics are used, as discussed above.¹⁴¹ Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out. Performing a DPIA¹⁴² prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing from a data protection perspective.

8.6 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

The deployment of biometric identification systems by a Humanitarian Organization may involve outsourcing work to local operators for project implementation on-site. These highly sophisticated technologies require the support of specialized technology providers. Humanitarian Organizations may also cooperate among themselves in sharing databases of biometric information (see above). State authorities (for example, law enforcement agencies) may apply pressure on Humanitarian Organizations to access biometric information held by them (for example, when people migrate and/or are forcibly displaced), either in bulk or for specific individuals.

¹⁴¹ See [Section 8.2.1: Legal bases for Personal Data Processing](#).

¹⁴² See [Section 8.7: Data Protection Impact Assessments](#).

In view of the above, it is crucial to define which parties actually determine the purposes and means of data Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). When the roles have been clearly defined and the corresponding tasks assigned, International Data Sharing across Humanitarian Organizations and/or national borders and/or private or public sector Third Parties should only take place if appropriate contractual clauses are concluded that set forth the responsibilities of the parties. It should also be carefully established whether any Data Processors engaged are in a position to fully comply with security and segregation requirements. This is particularly important for biometric technologies, when some Data Processors may manage work outsourced from multiple Data Controllers and, where such Data Controllers include both Humanitarian Organizations and authorities, the risks that the data sets may not be properly segregated should be carefully assessed. DPIAs, drafted prior to the Processing of Biometrics data, may be a suitable means of clarifying the roles of different parties engaged in the Processing.

8.7 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of data protection regulations and the specific risks, highlighted above, are addressed.

It is essential to carry out DPIAs whenever biometric information is processed by Humanitarian Organizations. DPIAs should clarify the Processing details and specifications, highlight the potential risks and possible mitigating measures, so as to determine whether biometric data should be collected and, if so, what kind of safeguards should be put in place. It is important to note that DPIAs should be conducted prior to the Biometrics Processing.

CASH TRANSFER PROGRAMMING

POSSIBLE USE

SUPPORTING LOCAL MARKETS

LIVING PEOPLE CHOICE

POSSIBLE USE

SUPPORTING LOCAL MARKETS

ALIVING PEOPLE CHOICE

POSSIBLE USE

SUPPORTING LOCAL MARKETS

IVING PEOPLE
CHOICE

TRANSPARENCY
AS TO HOW
MUCH AID
REACHES
BENEFICIARIES

CHAPTER 9

CASH TRANSFER PROGRAMMING

9.1 INTRODUCTION

Cash transfer programming is a promising tool for supporting processes of survival and recovery from Humanitarian Emergencies. The terms Cash Transfer Programming, cash and voucher assistance, cash-based interventions and cash-based assistance can be used interchangeably and are understood to encapsulate all types of cash transfer programming, i.e. both vouchers and cash, and all types of delivery mechanism.¹⁴³

Cash transfers maximize the respect for beneficiaries' choices and the trade-offs they face. The world of humanitarian response continues to use several different varieties of cash and voucher assistance, ranging from vouchers that have to be exchanged for specific products or services from specific suppliers, to cash transfers that are made conditional on beneficiaries meeting some kind of requirement, or unrestricted and unconditional cash transfers that can be spent on anything affected people require.¹⁴⁴

There are different forms of electronic cash assistance, such as electronic cash, which is value sent to beneficiaries that can be converted into hard cash or spent without restrictions (e.g. mobile money, pre-paid cards, bank transfers); and electronic vouchers, which are sent to beneficiaries (through smart cards or mobile phones) that can be exchanged with approved merchants for approved items, with restrictions on spending possible.¹⁴⁵ Hard cash is sometimes also used, as well as paper vouchers.

It is widely recognized that the effectiveness and appropriateness of humanitarian aid provided in cash depends on the situation (e.g. can individuals obtain the items they need in a particular situation?).¹⁴⁶ Although some concerns have been raised about Cash Transfer Programming (e.g. inflation of the local market), there

143 See Diagram of Key Cash Transfer Terminology, Cash Transfers Glossary, at: https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/092017_cash_transfer_programming_terminology_glossary.pdf.

144 Center for Global Development, Doing cash differently: How cash transfers can transform humanitarian aid – Report of the High Level Panel on Humanitarian Cash Transfers (September 2015) p. 11: <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf>.

145 European Commission, *10 common principles for multi-purpose cash-based assistance to respond to humanitarian needs*, March 2015: http://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf; DG ECHO Funding Guidelines, *The use of cash and vouchers in humanitarian crises*, March 2013: http://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf.

146 Paul Harvey and Sarah Bailey, *Cash transfer programming and the humanitarian system*, Background Note for the High Level Panel on Humanitarian Cash Transfers, March 2015: <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9592.pdf>.

is evidence supporting cash and voucher assistance as a “good value for money compared to in-kind alternatives.”¹⁴⁷

Research has shown that the greater use of humanitarian cash transfers where appropriate, without restrictions and delivered as electronic payments wherever possible, has benefits such as the following:¹⁴⁸

- providing crisis-affected people with choice and greater control over their own lives
- aligning the humanitarian system better with what people need
- increasing the transparency of humanitarian aid and the prevention of fraud, by showing how much aid actually reaches the target population
- increasing accountability of humanitarian aid, both to affected populations and to the tax-paying public in donor countries
- potentially reducing the costs of delivering humanitarian aid to make limited budgets go further
- supporting local markets, jobs and the incomes of local producers
- increasing support for humanitarian aid from local people
- increasing the speed and flexibility of humanitarian response
- increasing financial inclusion by linking people with payment systems.

However, a number of difficulties and challenges also exist. Using cash and voucher assistance in some Humanitarian Emergencies may not be an optimal solution (for example, in cases where the goods and services needed are not available, where local authorities oppose this type of humanitarian aid, or where the relevant market is at a risk of inflation).¹⁴⁹ Cash transfers are simply a tool to reach a programme objective, and so cash transfers are often part of broader humanitarian assistance programmes, including measures providing protection, sanitation or health services.¹⁵⁰ For Cash Transfer Programming to function, Humanitarian Organizations need to process individuals’ Personal Data. This often includes data about an individual’s or group’s socioeconomic status and vulnerabilities. This poses inherent privacy-related threats and risks associated with the collection and handling of beneficiaries’ Personal Data, in particular in light of the complex data flows they involve. The use of digital technologies for Cash Transfer Programming often requires the involvement of non-humanitarian third parties (e.g. domestic and international mobile network providers, financial institutions and financial intelligence units). This means that Humanitarian Organizations lose control over the data collected and the metadata generated by the Cash Transfer Programming.

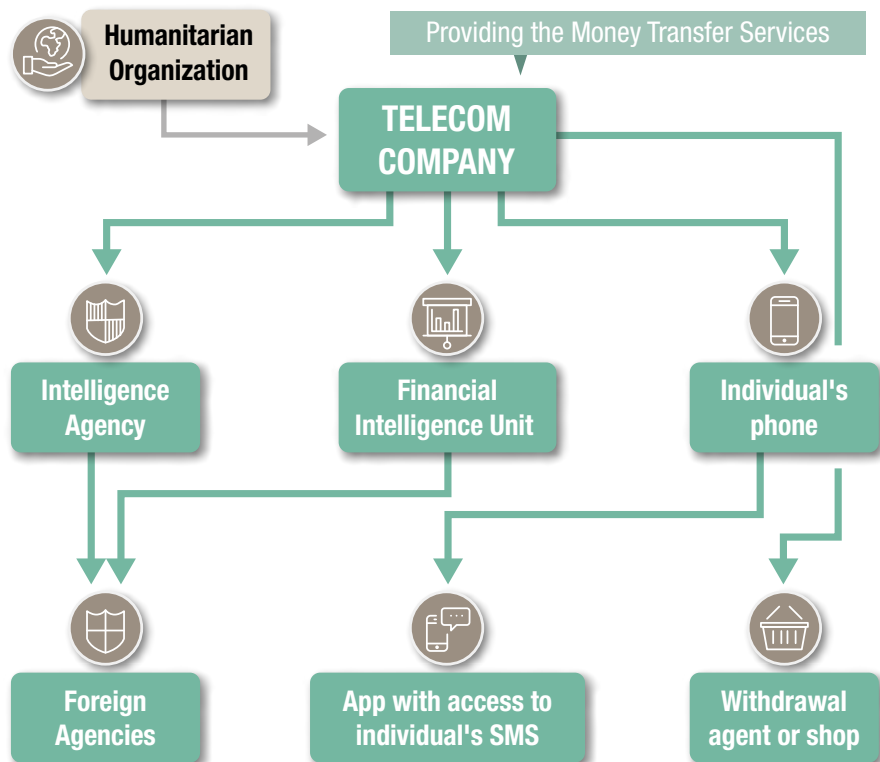
¹⁴⁷ *ibid.*

¹⁴⁸ ODI and Center for Global Development, *Doing cash differently: How cash transfers can transform humanitarian aid*, Report of the High Level Panel on Humanitarian Cash Transfers, September 2015, p. 8: <https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9828.pdf>.

¹⁴⁹ *ibid.*, p. 11.

¹⁵⁰ *ibid.*, p. 11.

How mobile money data can reach other parties



ICRC and Privacy International, Chapter 6: Cash Transfer Programming, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 73.

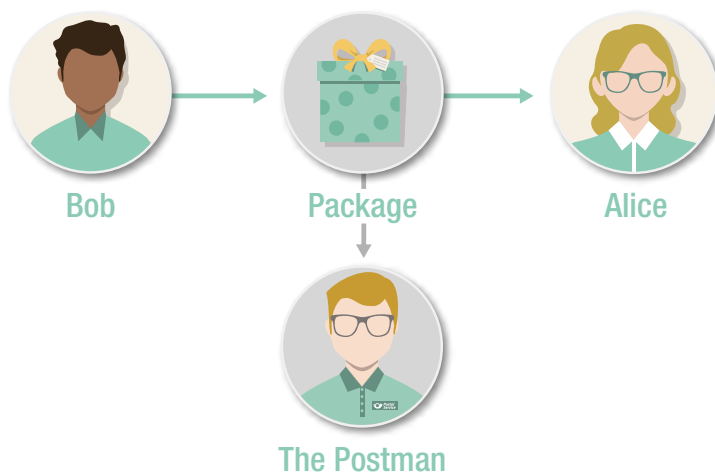
These data can then be used for non-humanitarian purposes (e.g. to profile potential customers). They can also be shared with external parties in order to comply with a legal obligation or under partnership agreements.¹⁵¹

In addition, a joint ICRC and Privacy International study stressed that, beyond knowingly collected and processed data, every single interaction generates what is known as metadata, i.e. data about data. This metadata is the inevitable result of the interaction with the system or service.

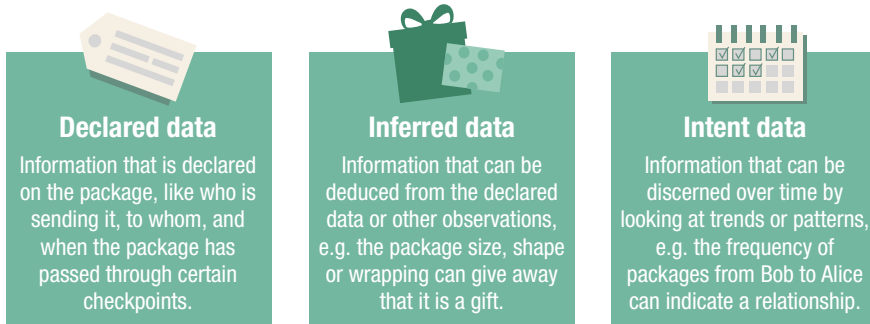
Finally, it is important to note that while the growing use of digital technology and connectivity is rendering previously “invisible” people “visible” to financial institutions, these digital identities and footprints can help to include people who

¹⁵¹ ICRC and Privacy International, “Chapter 6: Cash Transfer Programmes”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018.

Different types of data and metadata



The Postman might have an idea of what the package contains based on:



ICRC and Privacy International, Chapter 2: Processing data and metadata, *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 33.

were overlooked under previous programmes. However, this new visibility can expose beneficiaries to risks. The mere fact that they are seeking assistance from a humanitarian organization can reveal their affiliation with a particular group and expose them to discrimination. In other words, the inevitable visibility created by digital engagement can pose a threat in humanitarian situations. Digital visibility and profiling can become an instrument for financial discrimination, running counter the original purpose of the Cash Transfer Programming.¹⁵²

¹⁵² ICRC and Privacy International, “Section 6.1: CTP and financial inclusion: benefits and challenges”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, pp. 68–69.

9.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The inherent privacy-related threats and risks associated with the collection and handling of beneficiaries' Personal Data for Cash Transfer Programming can arise from inadequate organizational and technical data security measures. Humanitarian Organizations should also consider the long-term impact of the data generated, directly or indirectly, by Cash Transfer Programming. As Cash Transfer Programming makes use of existing services and systems including banks and telecommunications operators, Humanitarian Organizations may be required to collect data from beneficiaries in order to comply with Know Your Customer¹⁵³, SIM card registration¹⁵⁴ and other obligations to which such bodies are subject. Personal Data collected for Cash Transfer Programming can involve a variety of data sets that may not have been necessary for other types of humanitarian aid.¹⁵⁵ These data are shared with private entities to enable the distribution of financial aid.

Furthermore, careful consideration needs to be given not just to the data collected but also to the data generated, i.e. to the metadata produced through the practical arrangements of Cash Transfer Programming. Different legal and regulatory obligations apply to the collection, sharing and retention of such data. For example, in the case of mobile money, this includes data such as the sender's and recipient's phone numbers, the date and time of the financial transaction, the transaction ID, the location and size of the transaction, the store where it was conducted, and any agents involved at either end. Such data can be used to infer other information and intelligence, which could be used to profile, target and monitor users.¹⁵⁶ Humanitarian Organizations must therefore be aware of the ways in which data can be used to infer information about their beneficiaries' behaviours, movements, affiliations and other characteristics. The ability to draw inferences about beneficiaries is possible long after the programme ends.

153 Know Your Customer (KYC) is a process by which businesses check the identity of their customers in order to comply with anti-money laundering and anti-corruption regulations and legislation. See: PwC, *Anti-Money Laundering: Know Your Customer Quick Reference Guide and Global AML Resource Map*, PricewaterhouseCoopers, 2016, <https://www.pwc.com/gx/en/industries/financial-services/publications/financial-crime-guide-tool-and-global-financial-crime-resource-m.html>.

154 Kevin P. Donovan and Aaron K. Martin, "The rise of African SIM registration: The emerging dynamics of regulatory change", *First Monday*, Vol. 19, No. 2 (26 January 2014), Sec. IV, <http://firstmonday.org/ojs/index.php/fm/article/view/4351>.

155 Cash Learning Partnership, *Protecting Beneficiary Privacy, Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 4: <http://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf>.

156 ICRC and Privacy International, "Chapter 6: Cash Transfer Programming", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, pp. 73-75.

With an increasing number of Humanitarian Organizations opting for Cash Transfer Programming to provide assistance, there is a pressing need to consider the impact (e.g. will individuals receiving financial aid be subject to discrimination) and measures mitigating the risks associated with the Personal Data Processing needed to distribute this type of aid.¹⁵⁷

Data protection issues result from the fact that data are collected, stored and cross-matched by Data Controllers or Data Processors during cash assistance programming operations. Often, the data collected during Cash Transfer Programming relates to socioeconomic factors and vulnerabilities. The data are used to target assistance – either for a subset of the affected people (for needs assessment research), or for a wider group, potentially including people who do not ultimately receive cash transfers. For all recipients, the Personal Data collected during the process typically include the following: name, surname, mobile phone number, “Know Your Customer”¹⁵⁸ data, geolocation/other phone metadata and Biometrics. Humanitarian Organizations may also collect data related to socioeconomic factors or vulnerabilities for the purposes of targeting assistance. This data, once collected and stored, may enable Processing for other purposes and/or other types of data Processing, such as Data Analytics or data mining.¹⁵⁹

The complexity of the flow of data between Humanitarian Organizations and partner organizations using cash and voucher assistance also gives rise to data protection issues, which are dealt with in the section on data sharing below.¹⁶⁰

9.3 BASIC PRINCIPLES OF DATA PROTECTION

The basic principles of data protection constitute the baseline to be respected while engaging in any type of Personal Data Processing. These include the principle of the fairness and lawfulness of the Processing, the principle of transparency, the purpose limitation principle, the data minimization principle and the data quality principle.¹⁶¹

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

¹⁵⁷ *ibid*, p. 4.

¹⁵⁸ See Glossary and PWC, Know Your Customer: *Quick Reference Guide*: <http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html>.

¹⁵⁹ See [Chapter 6: Data Analytics and Big Data](#).

¹⁶⁰ See [Section 9.5: Data sharing](#).

¹⁶¹ See also [Chapter 2: Basic principles of data protection](#).

9.3.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data using one or more of the following legal bases:

- the vital interest of the data subject or of another person
- the public interest, in particular based on an Organization's mandate under national or international law
- Consent
- a legitimate interest of the Organization
- the performance of a contract
- compliance with a legal obligation.

Obtaining the valid informed Consent¹⁶² of beneficiaries in programmes using cash and voucher assistance can be challenging, due to the amount and complexity of information that would need to be provided to ensure the beneficiaries fully appreciate the risks and benefits of Processing. Moreover, merely interacting with the service inevitably generates metadata without the user's say.¹⁶³ As with other cases when Personal Data are collected as a prerequisite for assistance to be provided to beneficiaries, unless an alternative method of providing assistance is also made available, it can be argued that an individual in need of assistance has no real choice as to whether to give Consent or not and, accordingly, Consent may not be considered valid.

If Consent is not possible, then another legal basis could be used, as set out below. Beneficiaries should at least be informed individually or collectively as to the nature of the programme being provided, the legal basis for Processing, what data are being collected, by whom and why, whether providing the data is mandatory or voluntary, the sources of the data, how long it will be stored for, which Data Processors are involved, who else the data will be shared with, and their rights (including the right to redress).

Humanitarian Organizations should:¹⁶⁴

- aspire to obtain the active and informed Consent of beneficiaries for the use of their Personal Data when using cash and voucher assistance.
- only use alternatives to active and informed Consent where obtaining it is impractical or valid Consent cannot be obtained for other reasons set out herein. Legitimate reasons for not seeking active and informed Consent include urgency, or if the circumstances of the distribution make "active and informed Consent" meaningless.

¹⁶² See [Section 3.2: Consent](#).

¹⁶³ ICRC and Privacy International, "Chapter 6: Cash Transfer Programmes", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 21.

¹⁶⁴ Cash Learning Partnership, *Protecting Beneficiary Privacy, Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 13, *op. cit.*



In the far north of Cameroon, a woman consults the phone she uses to receive unconditional cash transfers.

- if possible, ensure that valid Consent can be provided or offer an alternative method of assistance for the individuals who are not comfortable with the data flows and/or stakeholders involved in the use of cash and voucher assistance.
- to the best of their knowledge given publicly available information, inform beneficiaries about the data and metadata which may be generated, collected and processed by third parties whose services and systems the Humanitarian Organizations is using (including KYC for banks and SIM card registration by telecommunications operators).

In light of the potential effectiveness of cash-based operations in disaster and emergency conditions and the rapidity of deployment if properly prepared in advance (e.g. if compared to in-kind assistance), the vital interests of the Data Subject or another person might constitute a plausible alternative legal basis for the relevant Processing when Humanitarian Organizations are unable to obtain the individuals' Consent. However, as always with this legal basis and as set out elsewhere in this Handbook, its use should be carefully considered.

Public interest could constitute a suitable legal basis for Processing data in the use of cash and voucher assistance where a mandate to carry out Humanitarian Action is established in national, regional or international law and where no Consent is obtained and no vital interests are triggered, as per the cases discussed above.

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. Such legitimate interests may include making humanitarian aid delivery more effective and efficient, preventing fraud and duplication of aid.

9.3.2 PURPOSE LIMITATION AND FURTHER PROCESSING

At the time of data collection, the Humanitarian Organization concerned must determine and set out the specific purpose/s for which data are processed.¹⁶⁵ The specific purpose/s should be explicit and legitimate and, in the case of Cash Transfer Programming, should involve the provision of assistance to enable affected people to access the goods and services they need.

The purposes of the Processing need to be clarified and communicated to individuals at the time of collection.

Personal Data may be processed for purposes other than those initially specified at the time of collection where the Further Processing is compatible with those purposes, including where the Processing is necessary for historical, statistical or scientific purposes. In order to establish whether Further Processing is compatible with the purpose for which the data were initially collected, attention should be paid to the following factors:

- any link between the purposes for which the data were initially collected and the purposes of the intended Further Processing
- the situation in which the Personal Data were collected, in particular, the relationship between Data Subjects and the Data Controller, as well as the relationship with the Data Processor
- the nature of the Personal Data
- the possible consequences of the intended Further Processing for Data Subjects
- the existence of appropriate safeguards
- the reasonable expectation of the Data Subjects as to possible further uses of the data.

When assessing the above, the humanitarian purposes of the data Processing should be given particular consideration.

Additional purposes that may be involved in the Processing by or of interest to commercial processors (e.g. financial institutions and mobile phone operators) should also be considered. This may potentially include: cross-checking lists of beneficiaries against lists of designated persons, retention of metadata for law

¹⁶⁵ See [Section 9.3.1: Legal bases for Personal Data Processing](#).

enforcement purposes, profiling beneficiaries for credit-worthiness, etc.¹⁶⁶ The following consequences would ensue should commercial Data Processors be obliged or in a position to process Personal Data for purposes other than the exclusively humanitarian purpose envisaged:

- It would become questionable whether the entities in question are indeed Data Processors, and not new Data Controllers, deciding on the means and purposes of Processing.
- The additional Processing may be incompatible with the initial purpose for collection and require a new legal basis. While a new legal basis may perhaps be found (such as compliance with a legal obligation to report designated persons), Humanitarian Organizations should carefully consider whether this is compatible with the neutral, impartial and independent nature of Humanitarian Action.

Contractual clauses in the Processing agreement should restrict Further Processing by Data Processors as much as possible.

In the case of Cash Transfer Programming, Humanitarian Organizations should be aware of the data and metadata processed by Data Processors whose services and systems they are using. These should be included in the DPIA to identify any areas that need to be regulated through contractual clauses.

EXAMPLE:

In the case of a system set up to disburse cash or voucher assistance by a Humanitarian Organization, to which purpose the individuals concerned have consented, the same system cannot be used to transmit participants' data to donors of the Humanitarian Organization for cross-referencing purposes.

Likewise, any data collected cannot be used by a financial institution to assess a beneficiary's creditworthiness and eligibility for financial services, including after they have received aid from a Humanitarian Organization.

9.3.3 DATA MINIMIZATION

The information collected for the purposes of cash assistance operations needs to be proportionate to these purposes. That is, only the Personal Data necessary for the identification of individuals should be collected and processed and any "excess" information that is not relevant to the identification purposes should not be collected and, if collected, should be deleted.

¹⁶⁶ ICRC and Privacy International, "Chapter 6: Cash Transfer Programmes", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, October 2018.

Given that many types of data are collected when using cash and voucher assistance, compartmentalization of the data is recommended as a way to meet data minimization requirements, with access being provided on a need-to-know basis. Additionally, contractual provisions could be provided against the Further Processing by commercial entities.

In assessing the application of the data minimization principle, it is also important to take into account the data generated as part of the Cash Transfer Programming by Data Processors, such as credit transaction metadata and mobile network metadata.

One possible option in programmes using cash and voucher assistance is for the Humanitarian Organization to transfer, when feasible, a unique identifier (from which the receiving entity cannot identify the final beneficiary) and the amount of cash to be distributed to the commercial service provider (e.g. bank or mobile network operator), so as to limit the risks to the individuals concerned. However, it is important to consider the limitations of these approaches, since programmes such as these depend on rigid systems provided by financial institutions, telecommunications operators and other relevant organizations. Likewise, it is important to recognize the limitations of current Anonymization techniques and the implications for re-identification, especially when data can be correlated with other sources to enable re-identification.¹⁶⁷

9.3.4 DATA RETENTION

Humanitarian Organizations are advised to ensure that beneficiary data are not held (whether by them or by Third Party Data Processors) for longer than is required to fulfil the specific purposes for which they were collected, unless retention is potentially useful for repeat distributions. The Personal Data of beneficiaries who have left the programme should be deleted both by the organization, its Data Processors, and any Third Parties that have had access to the data. The Humanitarian Organization should verify data deletion by the commercial service provider, as far as this is possible. Any information that is deemed necessary to keep at the end of a programme should only be kept if it is related to data for which there is a legitimate purpose, such as possible future programmes, auditing or reporting purposes, monitoring and evaluation. Ideally, and to the extent that this is meaningful, data retained for these reasons, should be aggregated and/or anonymized.

In considering data retention, Humanitarian Organizations should also consider the retention obligations that may apply by virtue of domestic law to some Data Processors, such as financial institutions, credit card companies and mobile phone network operators. These should be included in programme DPIAs and privacy policies.

¹⁶⁷ Larry Hardesty, “How Hard Is It to ‘de-anonymize’ cellphone data?,” MIT News, 27 March 2013, <https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>.

9.3.5 DATA SECURITY

In order to avoid potential misuse of the Personal Data collected and processed during Cash Transfer Programming, it is essential that adequate and proportionate security measures are implemented. Humanitarian Organizations are advised to implement appropriate technical and operational security standards for each stage of the collection, use and transfer of beneficiary data, and processes should be put in place for the protection of beneficiary Personal Data from loss, theft, damage or destruction; this includes back-up systems and effective means to respond to security breaches and prevent unauthorized access, disclosure or loss.¹⁶⁸

It is also advisable for the Humanitarian Organizations to protect “by design” the Personal Data they obtain from beneficiaries either for their own use or for use by Third Parties for each programme using cash or vouchers that they initiate or implement. This means that they should build privacy protections into the processes and mechanisms they use to implement cash and voucher assistance. Encryption or compartmentalization of information can be viable solutions to meet this need.

Humanitarian Organizations must take steps to inform themselves about the measures taken by potential Data Processors and other Third Parties on whose systems, services and infrastructure they rely prior to contracting them. Personal Data, at rest and in transit, as well as the infrastructure relied upon for Processing, should be protected by security safeguards against risks such as unlawful or unauthorized access, use and disclosure, as well as loss, destruction or damage of data. As part of their due diligence and DPIAs, Humanitarian Organizations should inform themselves about any publicly known security incidents experienced by Data Processors and other Third Parties on whose systems, services and infrastructure they rely, and what measures they have subsequently put in place to ensure the security and integrity of the data, at rest and in transit, and the infrastructure relied upon.

Data storage and potential International Data Sharing also need to be taken into consideration. For example, for refugees, there may be serious data protection risks associated with using a regional bank that has a branch or storage facility in the country of origin of the refugees, as the data may be requested by national authorities.

When selecting external Data Processors, the security measures they can guarantee should be a key factor.

¹⁶⁸ See [Section 2.8: Data security and Processing security](#).

9.4 RIGHTS OF DATA SUBJECTS

The right to information should be respected by ensuring that beneficiaries are informed individually or collectively as to the nature of the programme being provided, what information is being collected, by whom and why, and which Data Processors are involved. Humanitarian Organizations should be transparent about how they intend to use the Personal Data they collect and process. They should provide privacy notices accounting for the full data flow and data retention envisaged to beneficiaries who want more detailed information.

Adequate infrastructure and resources should be put in place to facilitate the rights to access, objection, deletion and rectification with regard to any programme using cash and voucher assistance. In this respect, it is advisable to incorporate complaint procedures into Personal Data Processing practices and internal data protection policies.

9.5 DATA SHARING

Personal Data Processing for Cash Transfer Programming may include data sharing with Data Processors and Third Parties when the data sets have been collected and processed by different Data Controllers or Data Processors (for example, if Humanitarian Organizations implementing a cash assistance programming system outsource individual identification in the field to on-site operators). It is important to take into consideration data protection requirements before sharing data and to note that “sharing” includes not only situations where data are actively transferred to Third Parties, but also those when they are made accessible to others (e.g. sharing a database which contains beneficiaries’ Personal Data).

Humanitarian Organizations may rely on partner organizations to collect data on their behalf, or on commercial organizations (such as financial institutions and mobile operators) involved in carrying out such programmes. These other organizations may be subject to a variety of legal and organizational requirements that lead them to share data with Third Parties (including regulators), which can include the following:

- “Know Your Customer” (KYC) obligations requiring the collection of more Personal Data than is strictly necessary for the purposes of providing assistance.
- obligations to cross-check KYC information against lists of designated persons established by local authorities, including entities potentially involved in a conflict or situation of violence. This process may potentially be monitored by public authorities, and may involve reporting obligations. This in turn gives rise to questions as to inclusion (i.e. can beneficiaries be excluded from an assistance programme on the basis of a match being found) and compromise the neutrality and independence of Humanitarian Action.

- collection of additional data as part of the process, such as geolocation or unique telephone identifiers and other mobile network metadata, when mobile phone operators are involved.
- requirements for SIM card registration.
- retention obligations incompatible with the information provided by Humanitarian Organizations at the time of collection.
- additional commercial purposes, such as profiling individuals for credit worthiness or advertising.
- additional obligations imposed on them by national law.

Privileges and immunities are also of great significance with respect to Cash Transfer Programming. In this regard, the provisions of [Section 10.9: Privileges and immunities and the cloud](#) should be considered for Cash Transfer Programming.

9.6 INTERNATIONAL DATA SHARING

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it in Cash Transfer Programming, as discussed in [Chapter 4: International Data Sharing](#). Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out.

Financial services are highly interconnected in a way that Humanitarian Organizations cannot control. The way in which data might travel within and outside national borders is affected by this interconnectedness, as well as by national laws, regulations and practices. For this reason, Humanitarian Organizations must discuss, with all institutions involved in the Cash Transfer Programming: (i) who their main partners are, nationally and internationally, and (ii) whether Cash Transfer Programming data can be kept outside any information exchanges.¹⁶⁹

9.7 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

The use of cash and voucher assistance by a Humanitarian Organization may involve local or international commercial service providers for project implementation. Humanitarian Organizations may also cooperate among themselves in sharing databases of the information collected via these operations. It is thus crucial to determine which parties actually determine the purposes and means of data

¹⁶⁹ ICRC and Privacy International, “Chapter 6: Cash Transfer Programmes”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 79.

Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers. When the roles have been clearly defined and the corresponding tasks assigned, data sharing across Humanitarian Organizations and/or national borders and/or third (private or state) bodies should generally be covered by appropriate contractual arrangements.

It should be remembered that although Personal Data may be protected while kept in the systems of Humanitarian Organizations which benefit from privileges and immunities under international law, the same data when transferred to Data Processors not enjoying those privileges and immunities may lose such protection. In addition, Data Processors may be obliged by local legislation to share data with government agencies and may even be obliged not to tell the Humanitarian Organizations from which the data originated about this data sharing.

9.8 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) need to be drafted and tailored to each programme utilizing cash and vouchers. Cash Transfer Programming may differ not only from organization to organization, but also within an organization itself. Each programme constitutes a separate data protection activity which should be subject to a DPIA. DPIAs will help the Humanitarian Organization to (a) identify the privacy risks to individuals, in particular, those deriving from the data flow and stakeholders involved; (b) identify the privacy and data protection compliance liabilities for the organization; (c) protect the organization's reputation and instil public confidence in the programme; and (d) ensure that the organization does not compromise on the neutrality of its Humanitarian Action.

It is recommended that Humanitarian Organizations analyse, document and understand the flow of beneficiary data for each programme they initiate or implement internally within their own organization or externally with others, identify the risks involved and develop risk mitigation strategies. Particular issues often associated with commercial service providers and relating to KYC regulations, mandatory reporting to national authorities, International Data Sharing, and potential cloud storage, need to be specifically assessed and weighed against the benefits of using cash and voucher assistance.

A template DPIA for cash transfer programming has been developed by the Cash Learning Partnership.¹⁷⁰

¹⁷⁰ Cash Learning Partnership, *Protecting Beneficiary Privacy, Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, p. 18: *op. cit.*



CLOUD SERVICE

POSSIBLE USE

STRONG COMPUTING POWER OVER SHORT PERIOD OF TIME

AGILITY IN SCALING UP

DATA HOSTED SAFELY AND SECURELY

CHALLENGES

LIMITED CONTROL OVER THE CLOUD SERVICE

INTERCEPTION OF SENSITIVE INFORMATION

FLEXIBILITY IN LOCATION

ENSURE ALL BACKUPS ARE DELETED ON REQUEST

POSSIBLE ACCESS BY CLOUD SOLUTION PROVIDERS

POSSIBLE ACCESS BY THE GOVERNMENT

CARRY OUT AUDITS



CHAPTER 10

CLOUD SERVICES

10.1 INTRODUCTION

The most widely used definition of “cloud computing” is the one published by the US National Institute of Standards and Technology (NIST),¹⁷¹ according to which, “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 NIST document defines three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four deployment models: public, private, community and hybrid cloud environments,¹⁷² although it should be borne in mind that new models are being developed all the time.

Cloud computing can facilitate and accelerate the creation and Processing of large collections of data and the production of new services and applications; it also makes deployment more agile. As humanitarian assistance is driven by information, this new, alternative data Processing paradigm has become a helpful tool for Humanitarian Organizations. Its benefits include access to large amounts of computing power over short periods of time, elasticity and flexibility about the location and flow of data, and cost savings.¹⁷³

However, Cloud Services can also bring risks and challenges for privacy and data protection. These can generally be grouped into two main categories: firstly, the lack of control over the data and secondly, the absence of transparency about the Processing operation itself. For Humanitarian Action the following risks are of particular importance:

- the use of services from unprotected locations
- the interception of sensitive information
- weak authentication
- data can be stolen from the Cloud Service provider, for instance by hackers
- possible access by government and law enforcement authorities.

¹⁷¹ US NIST SP 800–145, *The NIST Definition of Cloud Computing*, September 2011:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

¹⁷² European Data Protection Supervisor (EDPS), Opinion of 16 November 2012 on the Commission’s Communication on “Unleashing the potential of Cloud Computing in Europe”, p. 4: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

¹⁷³ Dara Schniederjans and Korey Ozpolat, *An Empirical Examination of Cloud Computing in Humanitarian Logistics*, Working Paper: <http://www.cba.uri.edu/research/brownbag/spring2013/documents/DaraS2013329paper.pdf>.

The data protection implications of cloud computing were highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Cloud Computing, adopted in Uruguay in 2012.¹⁷⁴

In addition, those Humanitarian Organizations that enjoy privileges and immunities under international law should be aware that outsourcing Personal Data Processing to a Third Party Cloud Service provider may put their data at risk of loss of such privileges and immunities. More details on the possible implications of privileges and immunities in a cloud environment are set out in [Section 10.9: Privileges and immunities and the cloud](#) below.

The three main types of Cloud Service models can be described as follows:¹⁷⁵

- Infrastructure as a Service (IaaS): an IaaS cloud offers access to the raw computing resources of a Cloud Service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.
- Platform as a Service (PaaS): a PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run on that platform or another instance of it. The platform may in turn be hosted on a cloud IaaS.
- Software as a Service (SaaS): a SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

There are also different types of cloud infrastructure. A private cloud is operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. In a public cloud, the services are rendered over a network that is open for public use. 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 models.

Each of these models has advantages and disadvantages. A public cloud is more accessible, as the information is stored offsite and therefore is available from anywhere via the internet. It offers the ability to scale up server capacity at short notice and can potentially save money. It can also be reviewed regularly with security and performance updates and improvements. On the other hand, as a public cloud is dependent on internet connectivity there is the risk of losing control

¹⁷⁴ See: http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10.

¹⁷⁵ Information Commissioner's Office, *Guidance on the use of Cloud Computing*, 2012, pp. 5–6: <https://ico.org.uk/for-the-public/online/cloud-computing/>.

over data because of unknown or unauthorized data transfer from one jurisdiction to another, false deletion of data, retention after the termination of services, hacking and security attacks. It is difficult to identify where the data are stored in a public cloud at a particular point in time, and deletion is almost never possible because of the many unmonitored back-ups. In addition, there are many privacy and confidentiality concerns, such as the fact that the Processing may be subject to a range of different applicable legislation which could mandate compulsory and unauthorized release of data and the potential for authorities to exercise jurisdiction.

In a private/internal cloud, data are kept within the organization's internal network, and therefore are not publicly accessible. It offers a more controlled environment and a limited number of users, so creating less risk of third-party disclosure. A private cloud can have the same usability, scalability and flexibility as a public cloud. Its disadvantages, though, are the cost and the fact that it may not have the latest performance and security upgrades/improvements.

A hybrid cloud allows organizations to determine which option to use, depending on the classification of information to be stored. Less sensitive information is usually sent to a public cloud, whereas more sensitive and confidential information is kept on a private or internal cloud. While this model offers cost savings, scalability, security and performance updates/improvements, it entails the same risks as a public cloud in terms of loss of control over data and unauthorized disclosure.

10.2 RESPONSIBILITY AND ACCOUNTABILITY IN THE CLOUD

The cloud client – provider relationship is a Data Controller – Data Processor relationship.¹⁷⁶ However, in exceptional cases the cloud provider may act as a Data Controller as well, in which case it has full (joint) responsibility for the data Processing and must comply with all relevant legal obligations for data protection. As the Data Controller, the cloud client (i.e. the Humanitarian Organization) is responsible for complying with legal obligations stemming from data protection law. Furthermore, the cloud client is responsible for selecting a cloud provider that complies with data protection legislation.

The notion of accountability expresses the direct compliance obligations that Data Controllers and Data Processors have under data protection law. This means that they must be able to ensure and demonstrate that their Processing activities comply with the relevant legal requirements, through the adoption and implementation of appropriate data protection policies and notices.

¹⁷⁶ See [Section 10.7: Data Controller/Data Processor relationship](#).

EXAMPLE:

When a Humanitarian Organization contracts with a cloud provider to store Personal Data in the cloud, it will remain liable to the Data Subjects for any breaches of data protection that the provider commits. It is therefore essential for the Humanitarian Organization to take the following steps before Personal Data are stored in a cloud:

- undertake a DPIA on the proposed storage of Personal Data in the cloud, and be prepared to cancel the project if the results show that this would cause undue risk for individuals' data protection;
- perform due diligence on the Cloud Service provider to ensure that the provider will use due care and takes data protection seriously;
- discuss data protection openly with the provider and assess whether the provider seems ready and able to fulfil their data protection obligations;
- carefully review the contract with the provider before signature and ensure that it contains adequate data protection language; and
- for Humanitarian Organizations enjoying privileges and immunities, ensure that such privileges and immunities are properly built into the cloud solution design, and are respected.

10.3 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

All data protection principles apply to Cloud Services; special attention is paid here to a number of issues that are of particular relevance.

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

10.3.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Before engaging a cloud provider Humanitarian Organizations need to demonstrate that one of the following legal bases is present:¹⁷⁷

- the vital interest of the Data Subject or of another person
- the public interest, in particular based on an Organization's mandate under national or international law
- Consent
- a legitimate interest of the Organization
- the performance of a contract
- compliance with a legal obligation.

¹⁷⁷ See [Chapter 3: Legal bases for Personal Data Processing](#).



Even when the vital interest of the Individuals is a sufficient legal basis for collecting Personal Data, there must also be a legal basis for placing the data in the cloud.

It is important in this regard to differentiate between the initial Processing of the Personal Data by the Humanitarian Organization and its Processing in the cloud. The Humanitarian Organization must have a legal basis for collecting and Processing the Personal Data in the first place, which can be any of the legal bases referred to in [Chapter 3: Legal bases for Personal Data Processing](#). In addition, there must be a separate legal basis for the Processing in the cloud. There should be a case by case assessment of each legal basis in each specific situation or humanitarian operation and whether it can be extended to the cloud, either as an “extra” legal basis or cumulatively.

EXAMPLE:

A Humanitarian Organization collects Personal Data from vulnerable individuals on the basis that it is in their vital interest. In order to provide humanitarian services more efficiently, it then wants to store the data in a private cloud, and to this end engages a Cloud Service provider. The vital interest of the individuals is a sufficient legal basis for collecting the Personal Data, but there must be a legal basis for placing the data in the cloud as well. Vital interest might not be a sufficient legal basis for placing the data in the cloud, since the humanitarian services could be performed without this; rather, the purpose of putting it in the cloud is to make the provision of humanitarian services more efficient. A possible legal basis for using the cloud provider could be that it is in the legitimate interest of the Humanitarian Organization and this interest is not outweighed by the fundamental rights of the Data Subjects whose data are being processed. This argument is strengthened by the fact that a private cloud is being used. A DPIA should be performed to confirm the legal basis.

10.3.2 FAIR AND LAWFUL PROCESSING

Personal Data must be processed lawfully and fairly. The lawfulness of the Processing refers to the identification of an appropriate legal basis,¹⁷⁸ while the requirement for fairness is a broad principle that is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations using Cloud Services should bear in mind that these Principles apply during all stages of Processing (i.e. collection, Processing and storage).

10.3.3 PURPOSE LIMITATION AND FURTHER PROCESSING

Humanitarian Organizations must determine and set out the specific purposes of Personal Data Processing. The purposes of the Processing need to be clarified and communicated to individuals at the time of collection.

Humanitarian purposes offer a wide basis upon which to justify Further Processing operations. Compatibility would, however, not be found if the risks for the individuals concerned outweigh the benefits of Further Processing. This depends on the particular case. For example, circumstances leading to a finding of incompatibility include risks that the Processing may run counter to the significant interests of the person to whom the information relates or of his/her family, in particular when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or their reputation.

In cloud computing environments, the cloud client is responsible for determining the purpose(s) of the Processing prior to the collection of Personal Data from the Data Subject and must inform the Data Subject accordingly. Based on the prohibition that the cloud client must not process Personal Data for other purposes that are inconsistent with the original ones, a Cloud Service provider cannot unilaterally decide or arrange for Personal Data (and its Processing) to be transmitted automatically to unknown cloud data centres. Furthermore, the cloud service provider cannot use Personal Data for its own purposes (such as, for example, marketing, carrying out research for other purposes or profiling).

Moreover, Further Processing that is incompatible with the original purpose(s) is also prohibited for the cloud provider and its sub-contractors. A typical cloud scenario may easily involve a larger number of sub-contractors. In order to mitigate the risk of Further Processing, the contract between cloud provider and cloud client should include technical and organizational measures and provide assurances for the logging and auditing of relevant Processing operations on Personal Data that are performed by employees of the cloud provider or the sub-contractors.

¹⁷⁸ See [Section 10.3.1: Legal bases for Personal Data Processing](#).

10.3.4 TRANSPARENCY

Transparency is an aspect of the fair and legitimate Processing of Personal Data and is also closely related to the provision of information to Data Subjects. The cloud client is obliged to provide Data Subjects, whose Personal Data or data related to them are collected, with detailed information; this includes the cloud client's identity, address and the purposes of the Processing; the recipients or categories of recipients of the data, including Data Processors, insofar as such further information is necessary to guarantee fair Processing; and information about their rights.

Transparency must also be guaranteed in the relationship(s) between cloud client, cloud provider and sub-contractors (if any). The cloud client can assess the lawfulness of the Personal Data Processing in the cloud only if the provider informs the client about all relevant issues. A Data Controller contemplating the engagement of a cloud provider should carefully check the provider's terms and conditions and assess them from a data protection point of view.

Another aspect of transparency in cloud computing is the fact that the cloud client must be informed about all the sub-contractors involved in the provision of the respective Cloud Service, not merely those with which it is in a direct contractual relationship, and the locations of all data centres in which Personal Data may be processed.

10.3.5 DATA RETENTION

Humanitarian Organizations are advised to ensure that Personal Data are not held (whether by them or by Data Processors) for longer than is required unless they have clear, justifiable and documented reasons for doing so; otherwise, data held by the organization and any relevant Third Parties should be destroyed. Deletion or destruction after completion of their Processing or a carefully structured data retention policy is recommended. When the purposes for which the Personal Data were collected have been achieved, then the Personal Data should be deleted both by the organization and any Third Parties that have had access to the data, unless the Third Party has Consent to hold that data.

Data should only be retained in Cloud Services if they are related to a legitimate Processing purpose. Legitimate purposes in this regard might include possible future programmes, monitoring and evaluation, whereas for research purposes anonymized or aggregated data might be appropriate. Only the minimum amount of data necessary should be retained, in accordance with the data minimization principle.

The responsibility to ensure that Personal Data are erased as soon as they are no longer necessary lies with the cloud client. Erasure of data is a crucial issue not only throughout the duration of a cloud computing contract, but also upon its

termination. It is also relevant if a sub-contractor is replaced or withdraws. In such a case, the cloud client might either request a certificate of destruction by the Cloud Service provider or a certificate confirming that the data were transferred to a new Cloud Service provider.

The principle of data erasure is applicable to Personal Data irrespective of whether they are stored on hard drives or other storage media (e.g. backup tapes). Since Personal Data may be kept at the same time on different servers at different locations, it must be ensured that each instance is erased irretrievably (i.e. previous versions, temporary files and even file fragments should also be deleted).

Secure erasure of Personal Data requires that either the storage media are destroyed or demagnetized, or that the stored Personal Data are deleted effectively. Special software tools that overwrite Personal Data multiple times, in accordance with a recognized specification, should be used. The cloud client should make sure that the cloud provider ensures secure erasure in the abovementioned sense and that the contract between the provider and the client contains clear provision for Personal Data erasure. The same holds true for contracts between cloud providers and sub-contractors.

10.4 DATA SECURITY

Data security measures can be legal, technical and organizational. Legal measures may include not only contractual arrangements, but also Data Protection Impact Assessments (DPIAs). A holistic perspective must be adopted, which takes the following phases of contracting for Cloud Services into account:

- assessing the decision to use cloud computing (via DPIAs and a “go/no go” decision by management)
- the Cloud Service procurement process, including due diligence on prospective Cloud Service providers that takes both legal and technical perspectives into account
- contracting (i.e. getting the right terms and conditions)
- operating, maintaining and decommissioning the service.

A comprehensive data protection strategy is recommended and attention should be paid to data protection issues in all phases before, during and after contractual arrangements. This should include an overall assessment of the contractual framework, including service level agreements (SLAs), general (non-data protection) clauses (e.g. applicable law, variations to the contract, jurisdiction, liability, indemnification, etc.), and the general principle of “parallelism in/outside the cloud” (e.g. having the same data retention period for cloud or non-cloud Processing).

When a Humanitarian Organization decides to contract for cloud computing services, it should choose a cloud provider that can give sufficient guarantees for technical security and organizational measures governing the envisaged Processing, and ensure compliance with those measures. Furthermore, a written contract with the Cloud Service provider must be signed, as there must be a binding legal act to govern the relationship between the Data Controller and the Data Processor. The contract must at a minimum establish that the Data Processor is to follow the instructions of the Data Controller and that the Data Processor must implement technical and organizational measures to adequately protect Personal Data, in accordance with the applicable data protection law.

In order to ensure legal certainty, the contract between the Humanitarian Organization and the Data Processor should also contain the following core data protection clauses:

- provision of information on the location of the data centres, the identity and location of sub-contractors, and on any subsequent changes to the nature of the Processing. This should include the subject and time frame of the Cloud Service to be provided by the cloud provider; the extent, manner and purpose of the Processing of Personal Data by the cloud provider; and the types of Personal Data processed.
- details about the cloud client's instructions to be given to the provider, with particular regard to the applicable SLAs and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).
- clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any Data Breach which affects the cloud client's data. Note that a security incident does not necessarily constitute a Data Breach.
- recognition of the obligation to process Personal Data only for the explicitly mentioned and specified purposes, and to delete data at the end of the contract. There must be specification of the conditions for returning the data or destroying them once the service is concluded. Furthermore, it must be ensured that Personal Data are erased securely at the request of the cloud client.
- confirmation, in case of a private cloud located outside the cloud client premises, that the data of the Humanitarian Organization are kept in separate servers.
- specification of security measures that the cloud provider must comply with, depending on the risks represented by the Processing and the nature of the data to be protected.
- a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to the data.
- an obligation on the provider's part to support the client in facilitating the exercise of Data Subjects' rights to access, correct or delete their data.
- an obligation on the provider's part to respect the cloud client's privileges and immunities, if applicable.

- a clause to the effect that Sub-Processors may only be commissioned on the basis of Consent that can be generally given by the Data Controller (cloud client), in line with a clear duty for the Data Processor to inform the Data Controller of any intended changes in this regard, with the Data Controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation for the cloud provider to name all the sub-contractors commissioned. It must be established that contracts between the cloud provider and sub-contractors reflect the stipulations of the contract between cloud client and cloud provider (i.e. that Sub-Processors are subject to the same contractual duties as the cloud provider). In particular, it must be guaranteed that both the cloud provider and all sub-contractors act only on instructions from the cloud client. The chain of liability should be clearly set out in the contract.
- arrangements for audits to be conducted during and at the end of the contract by the cloud client. The contract should provide for logging and auditing of relevant Processing operations on Personal Data that are performed by the cloud provider or the sub-contractors.
- a general obligation on the provider's part to give assurance that its internal organization and data Processing arrangements (and those of its Sub-Processors, if any) are compliant with the applicable national and international legal requirements and standards.

With regard to the technical aspects of data security, the following are some important considerations for Humanitarian Organizations to bear in mind:¹⁷⁹

- **Availability:** Providing availability means ensuring timely and reliable access to Personal Data. Availability in the cloud can be threatened by accidental loss of network connectivity between the client and the provider or of server performance caused by malicious actions such as (Distributed) Denial of Service (DoS) attacks. Other availability risks include accidental hardware failures both on the network and in the cloud Processing and data storage systems, power failures or other infrastructure problems. Data Controllers should therefore check that the cloud provider has adopted reasonable measures to cope with the risk of interferences such as backup internet network links, redundant storage and effective data backup mechanisms.
- **Integrity:** Integrity relates to the maintenance of data quality which should not be maliciously or accidentally altered during Processing, storage or transmission. For IT systems, integrity requires that Personal Data undergoing Processing on these systems remain unmodified. Personal Data modifications can be detected by cryptographic authentication mechanisms such as message authentication codes, signatures or cryptographic hash functions. Interference with the integrity of IT systems in the cloud can be prevented or detected by means of Intrusion

¹⁷⁹ Adapted from Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, WP 196, 1 July 2012, pp. 14-17: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Detection and Prevention Systems (IDS/IPS). These security tools are particularly important for the open network environments in which clouds usually operate.

- **Confidentiality:** In a cloud environment, encryption can significantly contribute to the confidentiality of Personal Data if applied correctly, although it does not render Personal Data irreversibly anonymous. It is simply a tool for the cloud client to ensure that the Personal Data they are responsible for can only be accessed by authorized persons who have the correct key. Personal Data encryption should be used for all data “in transit” and, when available, to data “at rest”. This applies particularly for Data Controllers who plan to transfer Sensitive Data. Communications between cloud provider and client, as well as between data centres, should also be encrypted. When encryption is chosen as a technical measure to secure data, it is also important to guarantee the security of the key. Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication). Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and sub-contractors.
- **Isolation (purpose limitation):** Isolation is an expression of the purpose limitation principle. In cloud infrastructures, resources such as storage, memory and networks are shared among many users. This creates new risks for data disclosure and illegitimate Further Processing. Isolation is meant to address this issue and ensure that data are not used beyond their initial original purpose and to maintain confidentiality and integrity. Isolation is achieved by adequate governance of the rights and roles for accessing Personal Data, and should be reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g. no user or administrator should be authorized to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for legitimate purposes (least privilege principle).
- **Intervenability:** Data Subjects have the rights of access, rectification, erasure, blocking and objection, as discussed below.¹⁸⁰
- **Portability:** The use of standard data formats and service interfaces by the cloud providers is very important, as it facilitates interoperability and portability between different cloud providers. Therefore, if a cloud client decides to move to another cloud provider, any lack of interoperability may make it difficult or impossible to transfer the client’s (personal) data to the new cloud provider, which is known as “vendor lock-in”. The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a Cloud Service. Data portability also refers to the ability of a Data Subject to obtain from the Data Controller a copy of data undergoing Processing in a commonly-used, structured, electronic format. In order to implement this right, it is important that, once the data have been transferred, no trace is left in the original system. In technical terms, it should become possible to verify the secure erasure of data.

¹⁸⁰ See [Section 10.5: Rights of Data Subjects](#).

The following are further IT security principles for Humanitarian Organizations to consider when moving to the cloud.¹⁸¹

10.4.1 DATA IN TRANSIT PROTECTION

Data transmissions must be properly secured against eavesdropping and tampering. This is relevant not only for connections between the premises of the organization and the cloud application, but also for data paths inside the service and for connections between the application and other services (API).¹⁸² A common solution is the encryption of network traffic, using network level traffic encryption (VPN),¹⁸³ transport layer security (TLS) or application level encryption. Due care must be taken to choose the correct protocols and implementation of encryption, as well as in the management of secret keys for the encryption itself. Dedicated fibre optic connections can also be used, where they are convenient and the situation allows it.

10.4.2 ASSET PROTECTION

Protecting assets in cloud situations is different from protecting them in on-site arrangements. Consequently, several specific points need to be considered when evaluating a cloud solution.

10.4.2.1 Physical location

It is important to know the physical location(s) of data storage in order to understand which legislation applies, but also the likelihood of specific threats, such as power and network outages, actions by hostile groups and organizations, and other country-specific threats. It is therefore important to obtain a detailed statement regarding the physical location of data centres and be aware that data exchanges between data centres in different locations can happen without the organization's knowledge.

For Humanitarian Organizations with privileges and immunities, it is also essential that the country in which data centres are stored has a legal obligation to respect privileges and immunities, and is known to respect them in practice.

¹⁸¹ The authors express their gratitude to ICT Legal Consulting for permission to use the material on cloud security. Adapted from UK National Cyber Security Centre, *Cloud Security Guidance: Implementing the Cloud Security Principles*, 17 November 2018: <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles>.

¹⁸² API – an application programming interface is a set of subroutine definitions, protocols and tools for building application software: https://en.wikipedia.org/wiki/Application_programming_interface.

¹⁸³ VPN – A virtual private network extends a private network across a public network, such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network: https://en.wikipedia.org/wiki/Virtual_private_network.

10.4.2.2 Data centre security

In Cloud Service arrangements, the physical security of data centres is fully controlled by the service provider; it is therefore important to have a clear idea of the security at the premises in which the data and applications are stored. This can be achieved by verifying the certifications (if any) obtained by the data centre and/or the contractual obligations underlying the relationship between the Cloud Service provider and the organization. The level of security guaranteed should match the level of security required by the application to be hosted in the cloud. Physical inspection could give useful information, but is unlikely to be possible in most cloud environments.

10.4.2.3 Data at rest security

The level of security for data at rest depends on the type of service required and other arrangements with the service provider. However, it is reasonable to assume that data will be stored in shared storage media, so a clear statement of the service provider about the protection level and how it is achieved is required, along with any related Third Party certification. However, it is recommended not to rely only on cloud provider security for data at rest, at least for most Sensitive Data, but to add additional layers of protection, such as encryption.

10.4.2.4 Data sanitization

Cloud environments are characterized by a high frequency of provisioning, deletion and migration of resources; in other words, data and applications can easily be moved around different parts of the shared infrastructure. If not correctly managed, this could lead to data disclosure, as other customers' applications will likely be run on the same hardware previously used by Humanitarian Organizations. Moreover, data could remain indefinitely in the cloud infrastructure. Measures should be taken to control this threat: using dedicated resources and/or verifying with the provider which measures are in place to erase or otherwise sanitize the data. The use of encryption, independently from the service provider, could offer an additional layer of protection.

10.4.2.5 Equipment disposal

Equipment disposal is closely related to the previous point and a fair level of confidence should be achieved that no data or information could remain stored or possibly be disclosed when hardware is decommissioned or disposed of. The cloud provider should give some guarantee that this requirement can be met or other measures must be adopted (i.e. encryption).

10.4.2.6 Availability

Cloud Services must offer the required level of availability; service level agreements (SLAs) are of paramount importance in this respect. The agreement should also be examined in terms of liabilities and responsibility. Verification of any publicly available information, which could help in ascertaining the actual reliability of the service offered, is recommended.

10.4.3 SEPARATION BETWEEN USERS

In a cloud environment, the service provider is responsible for guaranteeing user separation. However, it is important when evaluating a cloud provider, and even more so when the provider and the related technology are not widely known, to assess the technology used and gather any information that can help in understanding how the separation is ensured. The separation is affected by several factors, such as the service model, the deployment model (public versus private cloud) and other factors. To assess the effectiveness of separation measures, a penetration test can be useful, but only to a limited extent: it is valid only for the specific time when the test is carried out and it only gives an indication about known issues. A background check of previous incidents and their management by the provider can also be extremely useful.

10.4.4 GOVERNANCE

The service provider should have a proper security governance framework, as this is the basis to control and coordinate all security efforts, and to manage changes in threat and developments in technology. The provider should then demonstrate that it possesses the required elements that are typically associated with a C* level manager (e.g. CSO, CISO, CTO) in charge of cloud security; that it has a properly implemented framework for security governance; that security and security risks are included in general risk and financial management; and that it complies with regulations and legal requirements. Conformance with recognized standards should be assessed.

10.4.5 OPERATIONAL SECURITY

The cloud provision service must be operated in accordance with strict security requirements and security must be embedded in standard operating procedures. The main elements are:

- configuration and change management, to control what is in the production environment and related changes, to perform the required tests and receive proper authorization before making changes.
- vulnerability management, to assess, identify and correct security issues that can arise in services and infrastructure.
- monitoring, to detect anomalies, attacks and unauthorized actions that can undermine the security of the services.
- incident management: when an incident occurs, the service provider must be able to address it by taking adequate measures in order to mitigate, contain and properly correct the issue. This includes communications and reports to the customers and law enforcement authorities.

10.4.6 PERSONNEL

The Cloud Service provider must have in place measures to assess the trustworthiness of the personnel involved in the service management. Proper background checks and screening should be implemented for any privileged or sensitive role. Operators should be trained and must understand and acknowledge their responsibilities.

10.4.7 DEVELOPMENT

Service providers usually develop large parts of their infrastructure. They should employ best practices and industry standards to ensure that threats are evaluated during development; guidelines for secure design, coding, testing and deployment should be in place.

10.4.8 SUPPLY CHAIN

Cloud providers often use Third Party products and services to integrate or manage the services they offer. Any weakness along the supply chain can compromise the security of the entire Cloud Service and applications. The provider should describe how the third-party suppliers are screened; the acceptance process for services and products; how security risks are managed; how the security posture of the service providers is verified; and how spare parts, updates and other changes are verified. This process is made even more important by the fact that Cloud Services can be layered, relying on other service providers lower down the chain. If possible, verification of the suppliers should be performed or agreements should be in place to prevent the cloud provider from using Third Party suppliers not acceptable to the organization.

10.4.9 USER MANAGEMENT

Depending on the service offered, the authorization process may, in part, be managed by the cloud provider. This process should be assessed to verify its compliance with best practices, regulations and the organization's needs, in order to ensure secure access to management interfaces. These interfaces allow the performance of actions that can be considered equivalent, to a certain extent, to physical actions performed inside a traditional data centre; consequently, such actions need to be carefully guarded. Privileges should be fine-grained, so as to ensure the correct management of roles and privileges.

10.4.10 IDENTITY AND AUTHENTICATION

As with user management, access to any service interface should be strictly guarded. Implementation of identification and authorization processes should be assessed to conform to the security needs of the organization. Examples of different approaches are: two factor authentication, use of TLS client certificates, single sign-on systems, etc. The methods adopted must be kept up to date with developments in security and the growing sophistication of the threats.

10.4.11 EXTERNAL INTERFACES

When management interfaces are exposed, this increases the attack surface available to hostile entities. The security of those interfaces should therefore be assessed against this threat; the availability of solutions such as private networks or equivalent measures to access private interfaces should be assessed.

10.4.12 SERVICE ADMINISTRATION

The architecture and management of administration systems should be carefully designed and implemented, as these systems are highly valuable for attackers. Thus, a description of administration systems management and procedures can be useful to assess the security posture of the service provider.

10.4.13 AUDITS

The service provider should make available the results of independent audits or allow the organization to ask for an independent assessment or audit. Audit data regarding the services (performance, downtime, security incidents and so on) should also be available for scrutiny.

10.4.14 SERVICE USAGE

The organization must have a clear understanding of the interactions with the Cloud Service: interfaces, data exchanges, authorization process for users, administration, workloads and any other aspect that can influence the service considered as the sum of cloud and organization activities. A detailed assessment of data flow, processes and architectures must be conducted prior to implementing a cloud solution. Proper procedures must be designed and implemented, personnel must be trained, and operators should be provided with the requisite knowledge about the cloud solution, the usage, the relationship with the organization and other information related to correct use and management of the cloud solution.

10.5 RIGHTS OF DATA SUBJECTS

Data Subjects also have the rights of access, rectification, erasure and objection with regard to their Personal Data processed in the cloud.¹⁸⁴ The Humanitarian Organization must verify that the cloud provider does not impose technical and organizational obstacles to these requirements, even in cases when data are further processed by sub-contractors. The contract between the client and the provider should require that the cloud provider facilitates the exercise of the Data Subjects' rights and ensures that the same exercise of these rights is safeguarded in its relationship with any sub-contractor.

10.6 INTERNATIONAL DATA SHARING

By their very nature Cloud Services involve International Data Sharing of Personal Data with various parties located in different countries. Data protection law restricts International Data Sharing; Humanitarian Organizations should therefore ensure that the use of Cloud Services is in compliance with any laws to which they are subject, if any, and with their own internal policies. This means, for example, that any contract with a cloud provider should indicate how the provider complies with legal requirements concerning International Data Sharing (e.g. through the use of contractual clauses with its entities and with sub-contractors). Performing a DPIA¹⁸⁵ prior to International Data Sharing could further strengthen the lawfulness of such Processing from a data protection perspective.

10.7 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

As discussed in Section 4.5 above,¹⁸⁶ the relationship between a Humanitarian Organization that puts Personal Data in the cloud and a cloud provider that it contracts with to do so is, generally speaking, that of a Data Controller and a Data Processor. However, in practice these roles may be more difficult to categorize than is at first apparent, as this will depend on how much discretion the cloud provider has, and which should be defined in the agreement between the provider and the client. What is crucial is that these uncertainties should not affect the rights of Data Subjects, meaning that Humanitarian Organizations should be as transparent as possible about their use of Cloud Services and not allow cloud providers to disadvantage Data Subjects.

¹⁸⁴ See [Section 2.11: Rights of Data Subjects](#).

¹⁸⁵ See [Section 10.8: Data Protection Impact Assessments](#).

¹⁸⁶ See [Section 4.5: Data Controller/Data Processor relationship](#).

The use of Cloud Services by a Humanitarian Organization routinely involves the cloud provider hiring Sub-Processors. The contract with the provider should specify that Sub-Processors may only be used on the basis of Consent given by the Data Controller (i.e. the Humanitarian Organization). The Data Processor (cloud provider) should have a clear duty to inform the Data Controller of any changes in this regard, with the Data Controller retaining the option of objecting to such changes or terminating the contract.

10.8 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of data protection regulations and applicable risks are addressed. It is essential to carry out specific DPIAs tailored to cloud computing whenever there is interest in using Cloud Services.¹⁸⁷ DPIAs should clarify the Processing details and specifications, and also focus on the risks posed by it as well as on mitigating measures. In this respect, it is important to note that DPIAs should be undertaken prior to the use of Cloud Services.

10.9 PRIVILEGES AND IMMUNITIES AND THE CLOUD

Beyond the considerations above, Humanitarian Organizations benefitting from privileges and immunities should also consider that data placed in the cloud may jeopardize the protection of such privileges and immunities, unless specific legal, technical and organizational measures are put in place. This consideration is key, particularly given that in Humanitarian Emergencies, the privileges and immunities of a Humanitarian Organization may be the first line of protection for the Personal Data of vulnerable individuals, particularly in conflicts and other situations of violence.

Humanitarian Organizations should consider implementing the legal, organizational and technical measures suggested below, to ensure that their privileges and immunities are adequately protected in a cloud environment.

¹⁸⁷ See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

10.9.1 LEGAL MEASURES

- Data should be hosted and processed by external Data Processors exclusively in jurisdictions where the privileges and immunities of the organization are formally recognized by status agreements recognising the inviolability of files, archives, correspondence and communication wherever and by whomever the organizations' data are held, as well as immunity from every form of legal process. This legal protection should ideally be backed by a track record of such privileges and immunities being consistently respected.
- Data Processors and Sub-Processors should be bound by contractual obligation to notify any requesting authorities who seek to access data, that the data in question is covered by a Humanitarian Organization's privileges and immunities; to decline any requests for access by authorities, whether informal, administrative or through judicial process, and to re-direct the authorities' request to the Humanitarian Organization; to immediately notify the Humanitarian Organization of any request for access to its data, whether informal, administrative or through judicial process, the identity of the requesting authority and status of the request; and to assist the Humanitarian Organization with the provision of any information and documentation that may be necessary as part of any proceedings, whether informal, administrative or through judicial process, that may be required by the Humanitarian Organization in order to assert its privileges and immunities over the relevant data.

10.9.2 ORGANIZATIONAL MEASURES

- The data of the Humanitarian Organization should be held in segregated servers, and the data should be segregated from the data of other clients of the Data Processors and Sub-Processors.
- The servers hosting the data of the Humanitarian Organizations should be clearly marked with the emblem of the organization and the indication "Legally Privileged Information" should be marked on the servers.
- Where possible, the servers hosting the data of Humanitarian Organizations should only be accessed with the authorization of both the Data Processors and of the Humanitarian Organization.
- Staff of the Data Processor and Sub-Processors should be properly informed of the privileged status of the data, and trained on the procedure to follow in case of requests for access by Third Parties.

10.9.3 TECHNICAL MEASURES

- Data hosted in a cloud environment should be encrypted and encryption keys held only by the Humanitarian Organization.
- If the cloud solution envisaged is a SaaS, and the Data Processors and Sub-Processors need to manage the service offered, arrangements should be made to ensure that such Data Processors and Sub-Processors may access the system to manage it, run updates, fix bugs and support users, without ever having access to clear (unencrypted) data.

MOBILE MESSAGING APPS

POSSIBLE USE



CHALLENGES

NEED FOR CLEAR
GUIDANCE ON PROCESSING
BY HUMANITARIAN
ORGANIZATIONS OF
INFORMATION
GATHERED FROM
MESSAGING APPS



CHAPTER 11

MOBILE MESSAGING APPS

11.1 INTRODUCTION¹⁸⁸

In their daily work, Humanitarian Organizations rely on multiple communication channels, including formal (e.g. radio and television), informal, unofficial and direct means of exchanging information. To employ the most appropriate communication channels in a given situation, Humanitarian Organizations have to understand the cultural background and needs of a particular society affected by a crisis and their means of communication.

In this respect, where such apps are widely used, their deployment by Humanitarian Organizations is particularly attractive, because it allows immediate communication with people affected by crisis or conflict, and helps to coordinate internal tasks and actions efficiently. This type of technology can enhance the effectiveness and efficiency of Humanitarian Actions and reach populations in remote or inaccessible locations. However, messaging apps are often employed without due consideration of the risks relating to Personal Data protection.



Migrants charge their mobile phones at a temporary Wi-Fi hotspot in a makeshift camp near the San Giovanni railway station in Como, Italy, August 2016.

¹⁸⁸ This chapter is based on the report *Humanitarian Futures for Messaging Apps*, ICRC, The Engine Room and Block Party, January 2017: <https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html>.

Despite the great functionality offered by mobile messaging apps, their use may entail significant data protection risks. It seems that in practice, Humanitarian Organizations sometimes deploy them ad hoc, without following any formal procedures underpinned by risk analysis or considerations of long term sustainability and management. Rather, the focus is on the Humanitarian Organizations' pressing information and communications needs. Insofar as this approach fails to include risk analysis, it runs counter to the guiding principles of Humanitarian Organizations, such as accountability, appropriateness, "do no harm", and due diligence. As is the case with any other communication channel, the adoption of mobile messaging apps requires the careful consideration of their benefits and risks. Questions to be included in such an analysis depend on the specific circumstances of a particular situation. For example, security concerns about Personal Data of individuals in a situation of political violence may differ greatly from security concerns in a natural disaster.

Mobile messaging apps installed on cellular phones or other smart devices may pose risks to individuals' right to Personal Data protection. This is because apps provide not only the possibility to exchange data between users, but also to process, aggregate, and generate huge amounts of data (e.g. metadata, location data and contacts). Some data protection regulators consider that risks to Personal Data Protection result from a combination of the following factors: 1) users' lack of awareness about the types of data they actually process on a smart device; 2) absence of user Consent; 3) poor security measures; and 4) the possibility of Further Processing.¹⁸⁹

In line with the "digital proximity" imperative, i.e. Humanitarian Organizations seeking to be digitally where the beneficiaries are (just as they try to be physically), Humanitarian Organizations tend to deploy mobile messaging apps that are popular in a particular society at the time of a Humanitarian Emergency, such as WhatsApp, Facebook Messenger, Snapchat, Viber, Telegram and LINE. These proprietary cross-platforms are established service providers which may not be willing to customize their applications to meet the needs of Humanitarian Organizations. At the same time, deploying a less popular communication platform may exclude the people the organization is seeking to help.

The adoption of mobile messaging apps may also result in the Further Processing of collected data, including Personal Data. Mobile messaging apps make it possible to collect information online and may also provide new ways of analysing the available data. In other words, data and metadata collected via mobile messaging apps can help to triangulate information in new ways. In light of this and the probability of

¹⁸⁹ See Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices (WP 202, 27 February 2013).

Further Processing of Personal Data, it is important to consider the purpose for using a messaging application as well as the entities with whom the collected data will be shared. Humanitarian Organizations may then find they are unable to state confidently that users can destroy or remove data already submitted, because this could entail multiple negotiations with multiple parties.

Mobile messaging apps were primarily designed to allow private communication between individuals or small groups. This type of functionality could be used by Humanitarian Organizations to provide basic counselling or to obtain information from beneficiaries about incidents, ongoing conflict or particular needs. However these apps may also be used in Humanitarian Action to “broadcast” content to large numbers of personal contacts or followers. In particular, in situations where the number of the users is very large, mobile messaging apps may work as a one-way broadcasting channel (e.g. to announce the time and place for delivery of humanitarian aid or changed opening hours of a local clinic).

11.1.1 MOBILE MESSAGING APPS IN HUMANITARIAN ACTION

A messaging application (or app) is a software program that allows users to send and receive information using their mobile phones or other smart portable devices. The ease with which apps work has had a great impact on their popularity, public acceptance and continuously increasing demand. There are three key differences between communication through mobile messaging apps and communication through mobile-phone networks:¹⁹⁰

- Mobile messaging apps transmit and receive data using a Wi-Fi internet connection or a mobile data connection (unlike SMS messages, which are transmitted over conventional telephone networks).
- Mobile messaging apps can transmit or receive a much wider range of data types than is possible using SMS or even its multimedia-enabled successor, MMS. Mobile messaging apps have developed more similarities than differences over time and in addition to voice calls and text, messaging app users can also send and receive the following types of information: files, including photos, images and (in some cases) documents; audio recordings, including voice recordings that act in the same way as a voicemail message; data identifying their current location, based on their phone’s GPS sensor; live video calls (in some apps); and emojis (pictographic representations of emotions or specific objects).
- Mobile messaging apps can transmit end-to-end encrypted content. They may, however, also generate and keep large amounts of – unencrypted – metadata.

¹⁹⁰ ICRC, The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps* (January 2017): <https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html>.

Humanitarian Organizations have been adopting mobile messaging apps for reasons such as the following:¹⁹¹

- to target audiences (staff or beneficiaries) already using messaging apps
- to reduce communications costs
- to maintain reliable contact with people (whether staff or beneficiaries) in transit; to enable communication with people in environments where other communications methods are unavailable
- to increase the speed of communications
- to improve the security of digital communications as compared with existing methods of communication (where such apps offer end-to-end encryption of content)
- to facilitate information collection from or dissemination to hard-to-reach, remote or inaccessible areas
- to speed up data collection or increase efficiency
- to improve inter-office coordination.

Based on the considerations above, there are two separate areas of analysis to be distinguished from a data protection point of view:

- Personal Data Processing through the mobile messaging apps themselves
- Personal Data Processing by Humanitarian Organizations, of data collected through mobile messaging apps.

These are addressed, in turn, below.

11.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

11.2.1 PROCESSING OF PERSONAL DATA THROUGH MOBILE MESSAGING APPS

Communicating with individuals affected by Humanitarian Emergencies through mobile apps requires Humanitarian Organizations, in most cases, to install and use applications already used by the majority of the population. Individuals, or in other words, beneficiaries in most cases have already downloaded and installed such applications and consented to their data protection terms.

¹⁹¹ For a more detailed explanation of the reasons to adopt mobile messaging apps in Humanitarian Action, See *Humanitarian Futures for Messaging Apps*, ICRC, The Engine Room and Block Party, January 2017, *op. cit.*

By communicating with beneficiaries through mobile messaging apps, however, Humanitarian Organizations may suggest, whether directly or indirectly, that such means of communication are secure and that no harm is likely to arise for the beneficiaries in engaging with the Humanitarian Organization. It is important therefore, that, irrespective of the initial Consent given by the beneficiaries to the app provider to process their Personal Data, a clear analysis of the implications of such use is made by the Humanitarian Organization to ensure that no unexpected negative consequences are generated by their engagement. It is recommended to do this with a DPIA, which would take into account the considerations set out below. The outcome of the DPIA may be that only certain types of data can be collected or communicated through a particular app, or that a particular app may be used only in certain circumstances and not others. It may also be that the use of a particularly popular app may be inappropriate for the Humanitarian Organization, and that the Humanitarian Organization may want to use such an app only to notify individuals of its intention to communicate through another, more secure, app. In carrying out the assessment it is also important to note that messaging apps develop and change features fast, and there is no guarantee that a feature offered by an app will be available indefinitely, or that users are running up-to-date software, particularly in countries where encryption is restricted by law. Similarly, companies' policies and statements about data usage, security and privacy may be revised at a later stage. Organizations will often be unable to view technical details of the underlying code, so they may be unable to make a comprehensive assessment of how any such changes affect users' security or privacy. Organizations that use third-party providers to manage or process information should also prepare to engage with these risks. Changes in app features may require revision of the DPIA.

The difference between one-way and two-way communication with beneficiaries through apps should also be highlighted, as the latter often carries much higher risks (potentially more Personal Data may be transferred) and also raises issues of long term management/sustainability against expectation.

11.2.1.1 Potential threats

Data protection and privacy concerns arise in every area of a Humanitarian Organization's work, so organizations should evaluate particular risks when considering whether to deploy a messaging app or not. Of these, the primary concern is the prospect that unintended Third Parties access data collected by Humanitarian Organizations, for purposes that run counter to the neutral, impartial and independent nature of humanitarian work (e.g. access by local authorities, law enforcement authorities, groups driven by various interests or private entities).

These Third Parties could include:

- entities in refugees' countries of origin, including armed groups and authorities, who may wish to identify groups or individuals for the purpose of harming and/or targeting them

- entities with migration policy or security interests, who wish to understand and predict displacement trends and flows
- entities with an interest in surveillance for national security purposes
- hostile parties who wish to target Humanitarian Organizations and the people that they support and carry out violent attacks against them
- commercial entities that wish to conduct behavioural profiling of particular groups, which can lead to discrimination.¹⁹²

Concerns in this area have been acknowledged and supported by the International Conference of Privacy and Data Protection Commissioners, in its 2015 Resolution on Privacy and International Humanitarian Action:

“Humanitarian organizations 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.”¹⁹³

11.2.2 WHAT KIND OF DATA DO MESSAGING APPS COLLECT OR STORE?

There are three main protocols in the mobile messaging and encryption world: the Signal Protocol, MTProto and iMessage.¹⁹⁴

1. The Signal Protocol (previously known as both Axolotl and TextSecure) is used by Open Whisper Systems’ Signal Messenger, Facebook’s WhatsApp, Facebook Messenger (in secret conversations), Google Allo (in incognito mode), Skype (since mid-2018, in private conversations) and Viber (proprietary, modified implementation).
2. MTProto was developed and is used by Telegram (in secret chats).
3. The iMessage protocol was developed by Apple and is used in iMessage.

Each of these messaging protocols generate and process different kinds of data, and also protect message contents and metadata to various degrees.

¹⁹² Maria Xynou and Chris Walker, *Why we still recommend Signal over WhatsApp*, 23 May 2016: <https://securityinabox.org/en/blog/2016-05-23/why-we-still-recommend-signal-over-whatsapp-even-though-they-both-use-end-to-end-encryption>.

¹⁹³ International Conference of Data Protection and Privacy Commissioners, Adopted Resolutions, Resolution on Privacy and International Humanitarian Action, 2015: *op. cit.*

¹⁹⁴ ICRC and Privacy International, “Chapter 6: Cash Transfer Programmes”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 50.

Message content: Although some major messaging app companies state that their apps offer end-to-end encryption, meaning that they are unable to decrypt or read the contents of messages, other widely-used apps such as Facebook Messenger store all message content on their servers. Note that some apps offering end-to-end encryption include it only as an opt-in feature (such as Telegram, LINE and Facebook Messenger). This means that unless users are aware of the need to enable this feature in their settings, all message data may still be sent unencrypted. Communication with most bots on services such as Telegram is not end-to-end encrypted. It is important to note that although the content may be protected, metadata may not enjoy the same kinds of safeguards (see “Metadata” below).¹⁹⁵

User information: When users sign up for an app, they are asked to submit information about themselves (ranging from a phone number, in the case of most apps, to images, full names and email addresses in the case of apps such as WeChat and Facebook Messenger). Mandatory SIM card registration is enforced in many countries worldwide. In these countries, an app’s requirement to submit a phone number may in effect prevent individuals from using messaging apps anonymously. In parts of Latin America, users may also be required to register their handset number.¹⁹⁶ Many apps automatically access a user’s list of phone number contacts during sign-up to find other contacts that already have the app. In some cases, apps may store this data separately (WhatsApp, for example, confirmed in June 2016 that it stores contact list information).¹⁹⁷ Details of any groups to which the user belongs may also be stored in some cases.

Metadata: According to their terms of service, apps collect varying quantities of metadata, including sites and information accessed from within the app. Examples of metadata that could be obtained from a message include IMEI/IMSI (device and SIM identifiers), sender phone number, recipient phone number, message size, location data, time data, IP addresses, hardware model and web browser information.¹⁹⁸ Many app companies state that such data are retained on their servers, although they rarely clarify the length of time that data are retained, or if and how metadata are encrypted (even among apps that claim to have implemented end-to-end encryption). Although some messaging applications

¹⁹⁵ Lucy Handley, “Sheryl Sandberg: WhatsApp metadata informs governments about terrorism in spite of encryption,” CNBC, 31 July 2017, <https://finance.yahoo.com/news/sheryl-sandberg-whatsapp-metadata-informs-112540721.html>.

¹⁹⁶ GSMA, *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*, April 2016: www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf.

¹⁹⁷ Micah Lee, *Battle of the secure messaging apps: How Signal beats WhatsApp*, The Intercept, 22 June 2016: <https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/>.

¹⁹⁸ ICRC and Privacy International, “Chapter 6: Cash Transfer Programmes”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, p. 60.

on personal computers offer to obscure users' metadata using Tor hidden services (software that enables anonymous browsing),¹⁹⁹ this is not an option on the major messaging apps currently available. Instead, the most privacy-conscious apps, such as Signal,²⁰⁰ simply aim to collect as little metadata as possible.

Inferred data: Even with end-to-end encryption of content, a lot can be inferred from the metadata around messaging:

Researchers at MIT and the Université Catholique de Louvain, in Belgium, analyzed data on 1.5 million cellphone users in a small European country over a span of 15 months and found that just four points of reference, with fairly low spatial and temporal resolution, was enough to uniquely identify 95 percent of them.

In other words, to extract the complete location information for a single person from an “anonymized” data set of more than a million people, all you would need to do is place him or her within a couple of hundred yards of a cellphone transmitter, sometime over the course of an hour, four times in one year. A few Twitter posts would probably provide all the information you needed, if they contained specific information about the person's whereabouts.²⁰¹

Data shared with Third Party providers: Messaging app companies frequently state that they share users' Personal Data with other companies which provide services to enable the app to operate. However, they rarely state which companies they work with, what services they provide, what data they have access to, or how the data are processed and stored. Twilio, a third-party provider that works with some messaging app companies, provides limited transparency reports which indicate that it received 376 requests for data from international agencies in the first half of 2016 compared with 46 over the same period in 2015.²⁰²

Evidence that a user has installed an app on their phone: By accessing an individual's physical device, authorities could find physical evidence that a user has installed a particular messaging app. This could also potentially be accessed through other means – for example, in most cases users must associate an email address with their smartphone to download an app, creating a potentially traceable link between the app and other online activity.

¹⁹⁹ All the following use Tor hidden services (software that is designed to allow anonymous communication): Guardian Project, *What is Orbot?*: <https://guardianproject.info/apps/orbot/>; Security in a Box, *Guide to Orbot*, <https://securityinabox.org/en/guide/orbot/android>; Tor Project, *Tor Messenger Beta: Chat over Tor, Easily*, 29 October 2015: <https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily>; Joseph Cox, 'Ricochet', the Messenger That Beats Metadata, Passes Security Audit, 17 February 2016: <http://motherboard.vice.com/read/ricochet-encrypted-messenger-tackles-metadata-problem-head-on>.

²⁰⁰ Signal, *Grand jury subpoena for Signal user data*, Eastern District of Virginia, 4 October 2016: <https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/>.

²⁰¹ L. Hardesty, "How hard is it to 'de-anonymize' cellphone data?", MIT News, 27 March 2013: <https://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>.

²⁰² See Twilio, *Transparency Policy*: <https://www.twilio.com/legal/transparency>.

11.2.3 HOW COULD OTHER PARTIES ACCESS DATA SHARED ON MESSAGING APPS?

Other parties may be able to access data transmitted through messaging apps in a number of ways, including:

- A messaging app company (or a third-party provider that accesses app users' personal information) discloses message content or metadata that it stores on its servers, in response to a disclosure request from an authority in the jurisdiction where such data are stored.
- Another party gains unlawful or covert access to message content or metadata stored on a messaging app company's servers (through hacking) or accesses that information while it is travelling between the two actors (known as a "man-in-the-middle" attack). For example, tests by the University of Toronto's Citizen Lab in late 2013 indicated that the messaging app LINE was not encrypting content sent over 3G connections despite the fact that content sent over Wi-Fi was encrypted.²⁰³
- When a device (e.g. a mobile phone or computer) is seized, forensic tools can be used to access its metadata, including content and data that the user believed to be deleted.²⁰⁴ Extraction tools can be used to download data from mobile phones, including:
 - contacts
 - call data (who we call, when, and for how long)
 - text messages
 - stored files (photos, videos, audio files, documents, etc.)
 - app data (what apps we use and the data stored on them)
 - location information
 - Wi-Fi network connections (which can reveal the locations of any place where we have connected to Wi-Fi, such as our workplace and properties we have visited).

²⁰³ 3G networks are encrypted by default, but only at the level of the network provider, meaning that internet service providers (ISPs) and telecommunications companies can decrypt information sent over them. Citizen Lab, *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*, November 2013: <https://citizenlab.ca/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/>; Thailand's Government Claims It Can Monitor The Country's 30M Line Users: <https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/>.

²⁰⁴ ICRC and Privacy International, "Section 5.3 Other metadata", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018.

Some mobile phone extraction tools may also access data stored in the cloud instead of directly on our phones, or data we do not know exists or cannot access, i.e. deleted data.²⁰⁵

- Parties access messaging app content through other covert methods. These include accessing the SMS login codes sent to users when they sign up for an app by redirecting traffic on conventional mobile phone networks,²⁰⁶ or inducing users to install “malware” (short for malicious software) onto their phone which enables others to remotely gain access to that phone or data stored on it.²⁰⁷
- An individual is forced to hand over their physical device. End-to-end encryption only encrypts data in transit, not on the user’s device. If a party gains physical access to a phone or computer with access to a user’s messaging apps account (such as by compelling the user to unlock it), they may be able to access message content as well as details of apps that are installed on the device. In some countries, authorities consider merely installing apps such as WhatsApp as an indicator of subversive behaviour.²⁰⁸ Signal, Telegram and Snapchat all offer “self-destructing messages”, which are only visible on the sender and recipients’ phones for a limited time before being automatically deleted.
- A messaging app company allows an authority to directly access content or data transmitted over the app by building a secret feature into its code (known as a “backdoor”). For example, certain countries have reportedly threatened to fine messaging app companies that did not introduce backdoors into their code, specifically citing WhatsApp, Telegram and Viber.²⁰⁹ Other companies have publicly stated that they have refused requests from government agencies

205 Mobile Phone Extraction, explainer produced by Privacy International and Liberty as part of the joint campaign “Neighbourhood Watch: How policing surveillance technology impacts your rights”, available at: <https://privacyinternational.org/neighbourhood-watched>.

206 Frederic Jacobs, *How Russia Works on Intercepting Messaging Apps*, 30 April 2016: <https://www.bellingcat.com/news/2016/04/30/russia-telegram-hack/>; Operational Telegram, 18 November 2015: <https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.fivg48cl1>.

207 See for example, Iran Threats, *Malware posing as human rights organizations targeting Iranians, foreign policy institutions and Middle Eastern countries*, 1 September 2016: <https://iranthreats.github.io/resources/human-rights-impersonation-malware/>.

208 Electronic Frontier Foundation, *Your Apps, Please? China Shows how Surveillance Leads to Intimidation and Software Censorship*, January 2016: <https://www.eff.org/deepinks/2016/01/china-shows-how-backdoors-lead-software-censorship>; Maria Xynou and Chris Walker, *Why we still recommend Signal over WhatsApp*, 23 May 2016: <https://securityinabox.org/en/blog/2016-05-23/why-we-still-recommend-signal-over-whatsapp-even-though-they-both-use-end-to-end-encryption>.

209 Patrick Howell O'Neill, *Russian bill requires encryption backdoors in all messenger apps*, 20 June 2016: <http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/>.

to create backdoors.²¹⁰ There have also been ongoing attempts by intelligence agencies to enable them to access encrypted content.²¹¹

- If the group is set as “public” (i.e. anyone can join without being invited), these data could be accessed; also, in a messaging group such as on WhatsApp, every member of the group can extract the declared names of other members, their phone numbers and the messages they have sent.²¹²
- The protections used in messaging apps have also been compromised by flaws in SS7, the underlying telecoms protocols.²¹³ These flaws allow individuals to impersonate a phone number, create a duplicate account on a messaging app, and send and receive all messages destined for this number without the user’s knowledge.²¹⁴

11.2.4 MESSAGING APP FEATURES RELATED TO PRIVACY AND SECURITY

The following are relevant features to look for when choosing a messaging app to exchange information in humanitarian situations.

11.2.4.1 Anonymity permitted/no requirement for authenticated identity

Enabling users to communicate anonymously via a messaging app enhances their privacy, whereas requiring the use of real names, email addresses and authenticated identities increases the risk that individuals will be monitored or targeted. The less

²¹⁰ Jon Russell, *Tim Cook Says Apple Won’t Create Universal iPhone Backdoor For FBI*, 17 February 2016, <https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/>; Max Eddy, *What It’s Like When The FBI Asks You To Backdoor Your Software*, 8 January 2014: <http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software>.

²¹¹ For reference see: Privacy International, *Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages*, 29 May 2019. Available at: <https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages>.

²¹² V. Wadhwa, “WhatsApp Public Groups Can Leave User Data Vulnerable to Scraping”, VentureBeat, 3 April 2018, <https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/>.

²¹³ Today’s public switched telephone network (PSTN, i.e. the sum of all nationally, regionally or locally operated circuit-switched telephone networks) uses a signalling system called Signalling System No. 7 (“SS7”). SS7 is also the foundation of mobile telephony, used to route calls, SMS and other mobile services. For more details see: ICRC and Privacy International, “Section 5: Telecommunications and messaging”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018.

²¹⁴ Vijay, “How To Hack WhatsApp Using SS7 Flaw,” TechWorm (blog), 2 June 2016, <https://www.techworm.net/2016/06/how-to-hack-whatsapp-using-ss7-flaw.html>; John Leyden, “SS7 Spookery on the Cheap Allows Hackers to Impersonate Mobile Chat Subscribers,” The Register, 10 May 2016, Online edition, sec. Security, https://www.theregister.co.uk/2016/05/10/ss7_mobile_chat_hack/.

information a user is required to provide in order to use an app, the less information about them other parties may be able to access.

11.2.4.2 No retention of message content

User privacy is better served when the contents of messages are delivered to a user's device and deleted from the app company's servers after they are read. Apps such as Telegram, WhatsApp, Viber and Signal state that they do not routinely store messages and that they delete messages from their servers immediately after they have been delivered to their intended recipient(s). However, companies such as Skype retain message content on their servers after the user has read the message, without stating a maximum time limit after which they will delete the data.

11.2.4.3 End-to-end encryption

End-to-end encryption restricts the ability of Third Parties such as governments or adversaries to intercept communications between Humanitarian Organizations and their beneficiaries in a way that allows the message contents to be viewed. In this case, even if a company does retain content data, this will be in encrypted form and thus not legible to the company or to any Third Party seeking access to the data. Encryption thus restricts the type and amount of legible data that messaging-app companies can be compelled to disclose. Ideally, it should be deployed by default in both one-to-one and group chats. There are online resources which assess the levels of security offered by specific apps.²¹⁵

11.2.4.4 User ownership of data

It is essential that messaging-app users be regarded as the lawful owners of their personally identifiable data as well as the contents of their messages. This prevents messaging-app companies from using such data for commercial or other purposes without the explicit Consent of the user. This issue is addressed by national law in some countries and the topic may also be included in the messaging apps' terms-of-service agreements.

11.2.4.5 No or minimal retention of metadata

The less metadata messaging apps retain on their servers, the less data they can be compelled to disclose to governments or sell to commercial interests. Messaging apps such as Signal and Telegram claim not to retain any metadata on their users, although Telegram's claim is contested,²¹⁶ whereas most major apps under consideration state that they collect contact numbers, logs of activity on the app and location information.

²¹⁵ Electronic Frontier Foundation, Secure Messaging Scorecard: <https://www EFF.org/pages/secure-messaging-scorecard>.

²¹⁶ Jeremy Seth Davis, *Telegram metadata allows for 'stalking anyone'*, 30 July 2015: <https://www.scmagazine.com/home/security-news/telegram-metadata-allows-for-stalking-anyone/>.

11.2.4.6 Messaging-app code is open source

When the code which underpins a messaging app is open source, the app can be independently scrutinized to verify that it has no vulnerabilities to security threats or hidden surveillance functions such as backdoors. Ideally, an app will publish its entire codebase openly: messaging apps such as Signal and Wire are entirely open source, while apps such as Telegram and Threema publish only part of their code.²¹⁷

11.2.4.7 Company vets disclosure requests from law enforcement

It is critical that the company producing the messaging app rigorously vets and responds in a restrained manner to law-enforcement requests for user data. Ideally, they will provide information on their own behaviour in this regard, publishing regularly updated transparency reports that provide details about what requests they have received from which jurisdictions, and what types of information they have provided. At the time of writing, Microsoft²¹⁸ and Facebook²¹⁹ publish regular transparency reports that detail how many requests they receive and how much data they hand over to law-enforcement agencies, while Open Whisper Systems (the company behind Signal) provides more detailed descriptions of the small number of requests they receive.²²⁰

Additionally, it is important to consider whether an entity providing a messaging app is located in a country where the government has broad surveillance powers or a record of regularly flouting legal restraints on surveillance.²²¹

11.2.4.8 Limited Personal Data sharing with Third Parties

Although messaging apps will need to share some data with Third Parties (typically those playing some technical role in the data Processing) in order to facilitate the delivery of their services, it is critical that companies do not share Personal Data, and only share minimal, de-identified data when this is strictly necessary. Organizations should choose a messaging app that does not share any data with Third Parties other than that which is strictly necessary for the technical operation of the service – and seek to confirm this explicitly with companies before proceeding.

²¹⁷ For more on this topic, see Lorenzo Franceschi-Bicchierai, *Wickr: Can the Snapchat for Grown-Ups Save You From Spies?*, 4 March 2013: <http://mashable.com/2013/03/04/wickr/#3EwYsDKZ5kqh>.

²¹⁸ Microsoft, Law Enforcement Requests Report: <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report>.

²¹⁹ Facebook, Government Requests to Facebook: <https://govtrequests.facebook.com/about/>.

²²⁰ Open Whisper Systems, Government Requests: <https://whispersystems.org/bigbrother>.

²²¹ Useful sources for further research include: <https://www.digcit.org/>; <https://privacyinternational.org/advocacy>; <https://advox.globalvoices.org/>; and <https://www.eff.org/deeplinks>.

11.2.4.9 Restricting access through the device's operating system, software or specific security patches

Newer versions of mobile phone operating systems also include additional security features that, for instance, prevent apps from accessing data elsewhere on the device. Users can also choose to grant individual permissions or enable full-device encryption. However, these newer devices and operating systems are unlikely to be found in the areas in which Humanitarian Organizations operate. This means that unauthorized third parties may be able to access the data shared, as well as the metadata generated through the use of messaging apps, using the various means outlined above (section 11.2.3).²²²

11.2.5 PROCESSING OF PERSONAL DATA COLLECTED THROUGH MOBILE MESSAGING APPS

Once the beneficiaries engage in communications with Humanitarian Organizations through mobile messaging apps, Humanitarian Organizations will need to collect, most likely store on other platforms, aggregate and analyse the information provided.

It is key that this Processing also takes place in line with the data protection principles set out in Part I of this Handbook. A few selected principles, specific to the collection of data through mobile messaging apps, are considered below.

Communicating with communities in humanitarian situations always involves negotiating a range of complex questions, including:

- Do individuals need to give a Humanitarian Organization “permission” to add their details to a group or channel?
- How can an individual opt out of receiving the content? Is this made clear to them at the outset?
- How can people be made aware of who their Personal Data are shared with?
- If requests for support that fall outside the Humanitarian Organization's mandate are shared with another humanitarian agency, are there clear data-sharing protocols to cover this?
- How do people know how long their data will be kept, and for what purposes?
- How can all these issues be communicated in a way that is easy to understand, including for people with limited experience of technology?

Working with messaging apps adds a new layer of complexity to all these issues.

In their DPIAs, Humanitarian Organizations should include details of the various protocols and the degree to which each protocol protects content and metadata.

²²² ICRC and Privacy International, “Chapter 4.3: Other metadata”, in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018, pp. 61–62.

Doing so will allow them to assess which option is best for a given purpose (i.e. sharing sensitive information), and also the context in which it will be used (i.e. legal and political), as well as the profile of beneficiaries.

11.3 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data collected through mobile messaging apps using one or more of the following legal bases:²²³

- the vital interest of the Data Subject or of another person
- the public interest, in particular based on an Organization's mandate under national or international law
- Consent
- a legitimate interest of the Organization
- the performance of a contract
- compliance with a legal obligation.

In most cases, the Processing of Personal Data collected through mobile messaging apps may be based on Consent, vital interest or the public interest. If individuals have already communicated with a Humanitarian Organization by messaging app, or have given their telephone numbers to them, then Consent to receive messages can be assumed. Consent, however, must be informed, and it is key that Humanitarian Organizations provide the relevant information concerning the purpose, retention or further sharing of collected data, etc. as discussed in the relevant Section of this Handbook.²²⁴

Otherwise, messages concerning Humanitarian Emergencies can be assumed to fall within the vital interest of Data Subjects or to be in the public interest. These legal bases also require that information be given to individuals, which can be done by sending them a link to the relevant information notice in a message via the mobile messaging application used.

11.4 DATA RETENTION

Humanitarian Organizations need to set out in their information notices and data protection policies how long they envisage holding the data collected.

Some of the data entered into most messaging apps are retained and stored by Third Parties (messaging app companies), which in turn share some of that data with

²²³ See [Chapter 3: Legal bases for Personal Data Processing](#).

²²⁴ See [Chapter 2: Basic principles of data protection](#).

other parties – whether service providers that enable an app to function, or parent companies (as with Facebook and WhatsApp). It is therefore also worth pointing out in the Humanitarian Organization’s information notice that the data provided through the app will also be retained by the app provider and any Third Parties involved, under the responsibility of the app provider and governed by their data protection policies.

Humanitarian Organizations should also consider having a retention policy concerning the exchanges of information or “chats” themselves and delete the chat history at regular intervals to ensure data minimization.

11.5 DATA SUBJECT RIGHTS TO RECTIFICATION AND DELETION

As per Part I of this Handbook, Humanitarian Organizations should provide for mechanisms to facilitate the effective exercise of Data Subjects’ rights, and inform Data Subjects thereof, in their data protection policies.

While this may be not problematic with regard to the data extracted from the messaging apps by the Humanitarian Organizations, it may be difficult to state confidently that messaging apps allow users to destroy or remove data that they have already submitted, because this could entail negotiations with multiple parties (not all of whom are transparent about the data that they hold). It is recommended that this factor also be specified in the data protection policy.

11.6 DATA MINIMIZATION

Considering the limited control Humanitarian Organizations have with regard to data collection by mobile messaging apps, organizations seeking to use messaging apps should aim to minimize the amount of information that is submitted to them. Academic research focused on the US has also found that users of messaging apps are usually unaware of the privacy implications of installing and sharing data on messaging apps.²²⁵ Therefore, it is suggested that Humanitarian Organizations should provide incentives for crisis-affected individuals to share Personal Data that are strictly necessary to provide humanitarian aid.

225 Kelley P.G., Consolvo S., Cranor L.F., Jung J., Sadeh N., Wetherall D. (2012) *A Conundrum of Permissions: Installing Applications on an Android Smartphone*. In: Blyth J., Dietrich S., Camp L.J. (eds) *Financial Cryptography and Data Security*. FC 2012. Lecture Notes in Computer Science, vol 7398. Springer, Berlin, Heidelberg: http://dx.doi.org/10.1007/978-3-642-34638-5_6.

EXAMPLE:

Ahead of South Africa's municipal elections in August 2016, the non-profit Africa's Voices Foundation partnered with Livity Africa to evaluate the impact of Voting is Power, a campaign to encourage young people to vote and highlight issues that mattered to them.²²⁶

To do so, they used online surveys of young people (conducted via email and through WhatsApp and Facebook Messenger) and posts published on social media. WhatsApp and Messenger were selected as channels because of their popularity with young people (476 people were engaged through Facebook Messenger and 46 through WhatsApp). Africa's Voices Foundation felt that their use of WhatsApp groups encouraged conversations that would yield particularly useful feedback. Impact and Communications Officer Rainbow Wilcox said: "the data that can be gathered [through WhatsApp] is rich, authentic, and provides insights into sociocultural beliefs and behaviours."

However, Africa's Voices had concerns about privacy when using both Facebook Messenger and WhatsApp. "We sought informed consent and stored the data securely, but we cannot control how the data will be used in these platforms," Claudia Abreu Lopes, Head of Research and Innovation, said. "It was problematic because we asked for personal information such as voting and demographics. We have decided not to embark on a [similar] project again if the privacy risks are not well understood before it starts."

As suggested above, it is recommended that Humanitarian Organizations also consider having clear policies on deleting chats at regular intervals, once the necessary data have been extracted.

11.7 PURPOSE LIMITATION AND FURTHER PROCESSING

In most cases data collected through mobile messaging apps will be extracted and analysed by Humanitarian Organizations on other platforms. As part of the Humanitarian Organizations' data protection policies to be communicated to the Data Subjects, Humanitarian Organizations should also clearly specify the purpose of Processing.

²²⁶ Africa's Voices, Case Study: Livity South Africa: <http://www.africasvoices.org/case-studies/livity-south-africa/>.

This can be particularly challenging considering the flexibility of use and immediacy of communication offered by such solutions, as it is likely that in any one chat numerous issues will be raised by a Data Subject, with each issue requiring one or more follow-up actions. With this in mind, and considering the compatibility of humanitarian purposes, it is suggested that a general humanitarian assistance and protection purpose specification should suffice.

Again, as Processing by mobile messaging applications is beyond the control of Humanitarian Organizations, the fact that such applications may process data for different purposes, according to their own data protection policies, should also be mentioned in the Humanitarian Organization's data protection policy.

11.8 MANAGING, ANALYSING AND VERIFYING DATA

Making use of data processed through messaging apps in Humanitarian Action is a challenge. Greater numbers of people can now collect and share larger volumes of data with organizations, but this means the organizations need to ensure they have the capacity to manage, analyse and verify collected data.

Difficulties can arise in creating a workflow to manage and analyse the information received. The systems used by messaging apps are not interoperable with existing information-management systems or databases; manual transcription of individual messages into spreadsheets is often the only way to allow Humanitarian Organizations to analyse data in a way that would allow for effective decision-making.

Challenges also arise with regard to verifying information received through messaging apps. While this is an issue in many online channels,²²⁷ verifying content from messaging apps is made more challenging by the speed at which information can be sent, as well as by message volume and the range of data types that can be sent. News media and human-rights defenders have attempted to respond to these challenges through collaboration and efforts to produce resources and guidance on the issue. Some of these resources may also be useful to Humanitarian Organizations.²²⁸

²²⁷ The Engine Room, *Verification of social media: The case of UNHCR on Twitter*: <https://responsibledata.io/reflection-stories/social-media-verification/>.

²²⁸ See for example, Craig Silverman (ed.), *The Verification Handbook*, European Journalism Centre, <http://verificationhandbook.com/>; Various authors, *DatNav: New Guide to navigate and integrate digital data in human rights research*, The Engine Room, Benetech and, Amnesty International, 2016; <https://www.theengineroom.org/datnav-digital-data-in-human-rights-research/>; First Draft News Partner Network, <https://firstdraftnews.org/about/>.

Humanitarian Organizations engage in Further Processing in cases where the Personal Data collected via apps are managed, analysed or verified. Consequently, Humanitarian Organizations have to ensure that Further Processing of Personal Data operations is compatible with the initial purpose for which data was collected.

11.9 DATA PROTECTION BY DESIGN

If Humanitarian Organizations intend to develop a messaging app, they should consider implementing the principle of data protection by design, which requires the development of privacy-friendly systems and services both for technical solutions and organizational measures. Carrying out a Data Protection Impact Assessment (DPIA) is a way to implement the principle of data protection by design in practice. The client-server architecture used to store data should also give effect to the principle of data protection by design.

When deciding to develop its own app or platform, there are a few considerations for a Humanitarian Organization to keep in mind. First, promoting use of the app among the organization's beneficiaries will prove challenging. And second, app maintenance and security involves ongoing costs. All software, once it has been developed, requires regular updates as new vulnerabilities emerge. A Humanitarian Organization will need to consider whether it has the in-house skills and expertise to develop and maintain such an app or platform.²²⁹

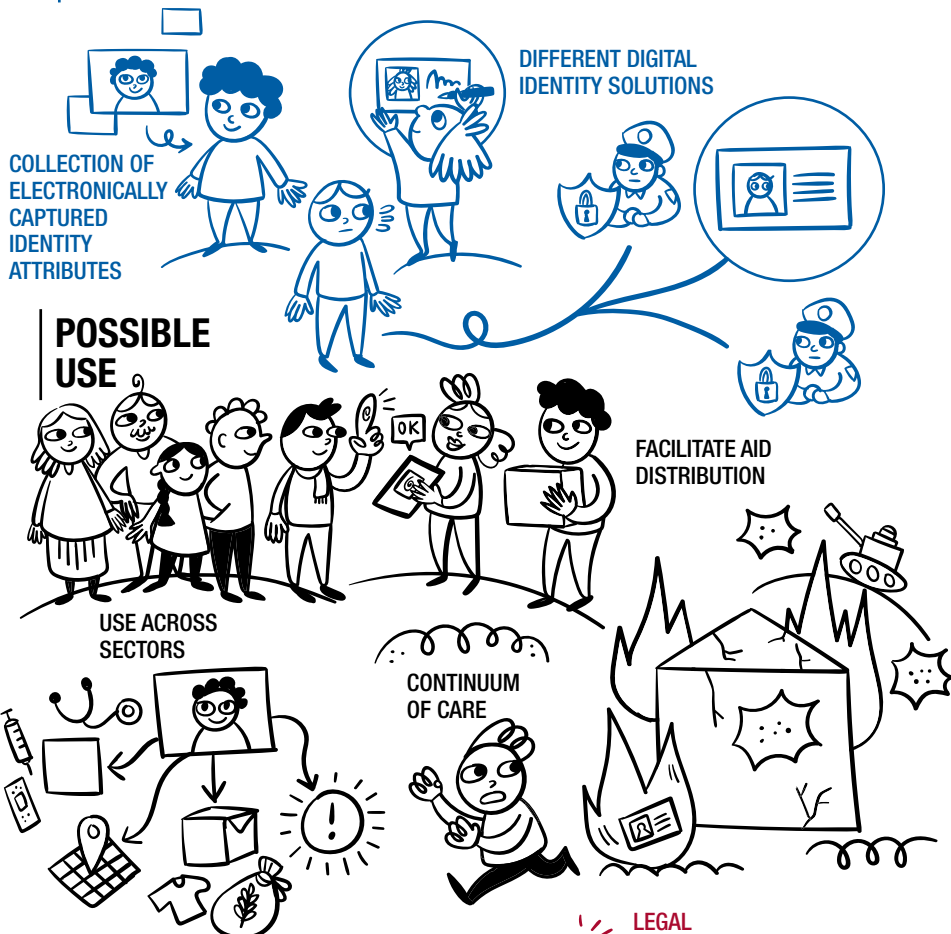
11.10 INTERNATIONAL DATA SHARING

It is also important to be aware that some services intersect, and they may overlap in terms of the entities and operating methods involved. In practice, this means that the data processing activities of social media networks and messaging apps must not, and cannot, be viewed as separate. Often, messaging apps are linked to social media networks directly (e.g. Facebook Messenger), or indirectly because they are owned by the same business group (e.g. WhatsApp is owned by Facebook). Here, services may share data for a variety of purposes.²³⁰

²²⁹ ICRC and Privacy International, "Chapter 5.4: Outsourcing, contracting, and using third parties", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018.

²³⁰ ICRC and Privacy International, "Section 4.1: Messaging apps and social media", in *The Humanitarian Metadata Problem: Doing No Harm in the Digital Era*, October 2018.

DIGITAL IDENTITY



CHALLENGES



CHAPTER 12

DIGITAL IDENTITY²³¹

231 The editors would like to thank Aiden Slavin (ID2020), Giulio Coppi (Norwegian Refugee Council), Dr Tom Fisher (Privacy International) and Robert Riemann (European Data Protection Supervisor) for their contributions to this chapter.

12.1 INTRODUCTION

Every human being has an identity. The right to identity is undisputed and recognized in international declarations and conventions.²³² But not all human beings have a way to prove their identity. In this regard, everyone should have a means to prove who they are through an identity tool.²³³ The form such a tool should take remains a matter of dispute. Yet no matter what its form – document, card, token, mobile app, or something else – it needs to be produced and managed. The mandates of humanitarian organizations frame their action, and this is particularly acute with digital identity as we will see in this chapter.

In most cases, Humanitarian Organizations need to use identity management systems to facilitate programmatic goals (e.g. a beneficiary management system set up to ensure aid is provided to the intended individual(s)).²³⁴ Some organizations have been involved in initiatives that aim to develop identity management systems that go beyond simply supporting a programmatic goal and, in practice, provide a legal identity²³⁵ (sometimes in a digital form) to those who lack identification documents and who, because of that, can be made “invisible, discounted, and left behind”.²³⁶ Sometimes, however, an identity tool that was initially designed and deployed to support programmatic goals shifts with time toward a broader use (such as to prove someone’s legal identity).

Against this background, this chapter analyses the data protection implications of setting up a Digital Identity management system for beneficiaries. The discussion covers, among other issues, the way in which Humanitarian Organizations collect and store data in such a system and how they manage information about participants, users and/or beneficiaries.

²³² See for example: Universal Declaration of Human Rights, Art. 6, and UN Convention on the Rights of the Child, Art. 7.

²³³ See SDG target 16.9: “By 2030, provide legal identity for all, including birth registration”: <https://sustainabledevelopment.un.org/sdg16>.

²³⁴ USAID, *Identity in a Digital Age: Infrastructure for Inclusive Development*, USAID, 2017, p. 1: https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf.

²³⁵ Throughout this chapter, the expression “legal identity” follows the UN operational definition of the term: “Legal identity is defined as the basic characteristics of an individual’s identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. This system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death. In the case of refugees, Member States are primarily responsible for issuing proof of legal identity. The issuance of proof of legal identity to refugees may also be administered by an internationally recognized and mandated authority.” UN Legal Identity Agenda: <https://unstats.un.org/legal-identity-agenda/>.

²³⁶ USAID, 2017, p. 1.

Term	Objectives	Typical characteristics	Examples
Functional identity	Enables a specific service (function) to authenticate participants.	Contextual, duplication of information.	Every individual can have multiple functional identities and these can be transnational, such as student ID, voter ID or food distribution programme ID.
Foundational identity (legal identity)	Provides a legal identity to a broad population as a public good without specifying a specific service. It allows individuals to prove who they are. The issuer of such an identity is considered a trusted source of identity – sometimes referred to as an authoritative source of identity.	Generates a legal identity that can be referenced by others. Within its given scope, every person can have only one such identity. However, the same person may have several legal identities (e.g. passports issued by different countries).	Typically government-based and covering the whole population of a country, ²³⁷ such as social security number, a birth certificate or an Aadhaar number (a 12-digit number that, in India, uniquely identifies people based on their biometric and demographic data).
Conceptual identity (personal identity)²³⁸	Defines an individual's identity in relation to others within a given societal structure, determining how they view themselves and how they are perceived by the society around them.	Intangible, variable and heavily defined by personal and societal perception.	Defining attributes (such as ethnicity, sexuality, religion or political orientation), according to which individuals define themselves and are defined by others within their society.

To start the discussion, it should be noted that there is no universally accepted definition of the term “Digital Identity”, although it can generally be agreed that Digital Identities consist of “a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions”.²³⁹ As a multi-faceted concept, however, Digital Identity can relate to a number of other important concepts, such as identification, functional identity, foundational identity, and personal identity.²⁴⁰ Since these terms are used throughout this chapter, a simplified explanation of each is given in the table above.

²³⁷ USAID, 2017, p. 12.

²³⁸ This chapter will not address conceptual identity as this cannot be encompassed by an identity system.

²³⁹ World Bank Group, GSMA and Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, World Bank Group, GSMA and Secure Identity Alliance, 2016, p. 11: <https://www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation/>.

²⁴⁰ J. Donner, “The difference between digital identity, identification, and ID: Caribou Digital’s style guide for talking about identity in a digital age”, 19 December 2018: <https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563>.

In view of these different types of identity, it is important for Humanitarian Organizations to clarify from the outset whether they require a functional or a foundation identity from beneficiaries, since this choice affects the design of the identity system and the associated management processes (e.g. collaboration with a third party, links to other existing systems, etc.). Often, legal constraints will drive decisions concerning the design of the identity system.

12.1.1 AUTHENTICATION, IDENTIFICATION AND VERIFICATION: WHO ARE YOU AND HOW CAN YOU PROVE IT?

Humanitarian Organizations do not always need to know someone's legal identity. This is true, for example, when the purpose of the interaction is to provide aid. Consequently, before developing a Digital Identity system, Humanitarian Organizations need to identify what information they need from beneficiaries for a specific humanitarian programme. Here, there is an important distinction to be made between authentication, identification and verification.

Identification answers the question: "Who are you?" But when setting up an identity management system, organizations should start by asking a different question, namely: "What do I need to know from that person to provide aid or protection?" Knowing who the person is can be important in some cases. For instance, when reuniting unaccompanied minors with their parents, it is critical to ascertain that the alleged parents are indeed who they purport to be. But quite often – possibly in most cases – it is enough simply to know that the person is entitled to access a service because they meet a certain criterion or have a particular set of attributes (e.g. they can prove they are under 12 in order to receive a particular vaccine). This is also known as authentication – or being able to prove a claim of who you are.

Even when Humanitarian Organizations only need authentication, they should carry out a verification process when registering beneficiaries in the identity management system. Verification, therefore, is the act of checking someone's identification (such as confirming a person's name on their identity document) or some of their identity attributes (such as confirming that a person is a member of the community that will receive aid by checking with the community leader). When a simple authentication system is used to ensure aid is delivered to affected individuals, verification at the time of enrolment can help to ensure that the people who were entitled to receive it were the ones registered. It should be noted, however, that some aid services may not need verification at all. This is true, for instance, when a Humanitarian Organization makes information available on an online platform where anyone can register.

When Humanitarian Organizations enrol and register beneficiaries, some data about them will need to be collected and stored in the identity management system. As will become clear below, deciding what attributes need to be recorded, and for what purpose(s), is a key decision from a data protection perspective. In particular, only attributes that are necessary to achieve the activity's purpose (e.g. supporting

the delivery of aid) should be collected. For example, in most cases, an organization would probably not need to store a copy of an identity document to record the fact that a registered person was verified to be a minor. Once enrolled, the beneficiary may receive some record of their identity, such as an attestation, a card, a pin code or a digital certificate they can access and manage on a mobile device. There is no need for further verification at the point of delivery, since the beneficiary already has proof that they are entitled to access the service in question.

12.1.2 DIGITAL IDENTITY

Digital Identity is a set of attributes stored digitally that uniquely describe a person in a given context (see the types of identity described previously: functional, foundational, and conceptual). In some cases, individuals could have more than one, and potentially hundreds of Digital Identities, each serving as a functional identity. This type of system would allow beneficiaries to access services, assistance or protection in a similar way to a username and password access model or a token system, without having to prove their legal identity.

In other cases, however, organizations may need to distinguish one individual from another with a high degree of certainty, and perhaps have only one Digital Identity for each person. In these scenarios, the identity system should allow a Digital Identity to be linked to a physical person. The aim here is to make it easier to distinguish between individuals, for instance when the organization is providing personalized aid (e.g. health care). Yet even when such a link is necessary, the organization might not need to obtain legal identity documents from beneficiaries. For instance, people might be able to register with their name only, without needing to confirm that the name they have given matches their legal identity (e.g. by checking it against their birth certificate or other identity document).

Lastly, there may be cases where the Humanitarian Organization needs a system that also allows it to ascertain and verify the individual's legal identity. This is very similar to the previous case, except that a legal identity document will be required in order to formally identify the person in question.

In summary, these are the main steps that a Humanitarian Organization should follow when setting up a Digital Identity management system:

- First, the organization decides what it needs to know about the affected people so it can implement a specific humanitarian programme. This will determine whether identification is required or whether authentication alone is sufficient. From a data protection standpoint, the latter option should be preferred wherever possible.
- Second, the organization determines, based on programme needs, whether it requires a functional or foundational identity, bearing in mind that only a handful of Humanitarian Organizations have a mandate to establish and/or manage foundational identities, and only for specific purposes.

- Third, the organization designs a verification process to cross-check the information provided at the enrolment stage. Depending on the chosen identity system, it can involve no particular formality, some due diligence, or an authoritative legal document. The organization should also determine whether or not it needs to retain the information assessed in the verification phase.

12.1.3 SYSTEM DESIGN AND GOVERNANCE

Once the Humanitarian Organization understands its objectives (authentication, identification and verification), it needs to decide how the Digital Identity system will be designed to achieve its intended purposes, and how it will be governed. The Humanitarian Organization (or other body) can control the system centrally, or control can be shared across multiple parties in a decentralized way.²⁴¹ Some current initiatives aim to give individuals control over their own identity systems by deciding who can access their identity credentials and when. In this sense, the governance structure is sometimes influenced by where the data will be hosted. When multiple parties access the same system, for instance, there needs to be a shared platform. Likewise, when efforts are made to shift control to individuals, it may be possible to allow them to store their credentials on their own devices or to use a service provider of their choosing.

The following decision tree summarizes the questions that Humanitarian Organizations should answer, and the factors they should consider, when deciding whether to implement an identity system:

1. Identity system type

- Can you rely on authentication only, or do you really need to identify the beneficiaries?
- Are you aiming to generate functional or foundational identity? (Remember: only some organizations have the mandate to generate foundational identity).
- Do you need to verify the information at enrolment? If not, is a system without verification acceptable? If so, does verification require a formal, legal identity document (or is a simpler form of verification acceptable)? Do you need to retain the information assessed during the verification process?

2. Design choices

- What information should be stored? By whom? And where?
- Note that verifying a particular attribute (such as nationality, to determine whether the person is eligible for inclusion in a humanitarian programme)

²⁴¹ The difference between decentralized and distributed architecture and a federated identity system is described in detail in the literature. While this is an important point, it is beyond the scope of this chapter and will therefore not be discussed here. For a more detailed description of decentralized identity, refer to the following sources: Digital Identity Foundation (<https://identity.foundation/>), World Wide Web Consortium (<https://w3c-cg.github.io/did-spec/>) and World Economic Forum (http://www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf).

does not mean that this information has to be stored in the identity system. The system can simply confirm that a person has the necessary attribute without further details.

- In some cases, there may be no need for verification in the first place. This applies, for example, to a generally accessible digital service, where an account can be created freely without disclosing any personal information, or to cases where an individual's mere presence in a place where people are displaced entitles them to access aid (when cards are distributed without collecting information, for instance).
- How will the data be controlled and governed? Who needs to access what information, at what point, and for what purposes?

12.1.4 DIGITAL IDENTITY IN THE HUMANITARIAN SECTOR: POSSIBLE SCENARIOS

The following four scenarios shed light on the interplay between various Digital Identity systems in the humanitarian sector.

Scenario 1: A Humanitarian Organization issues an identity credential (for example, a registration card or document) to a registered beneficiary of aid. In this scenario, the beneficiary – a Data Subject – would use a functional identity, which enables them to receive aid. In some situations, however, such an identification system could be accepted as a proof of who the beneficiary is – in other words, as a foundational identity (see scenario 4). Yet under some humanitarian programmes, individuals only have to authenticate to prove that they are legitimately entitled to access certain aid services, without the need for identification.

Scenario 2: A Humanitarian Organization offers multiple services to beneficiaries. In order to provide these services, each unit of the organization needs to have access to a certain part of the data collected from beneficiaries. For example, to provide in-kind aid, the unit may need to access aid distribution records linked to the beneficiary. Another unit, meanwhile, may need to access medical records to provide a follow-up treatment, while a third unit may need information about the individual to restore family links.

Scenario 3: Several Humanitarian Organizations provide multiple services to beneficiaries through a unified identity system. Under this type of shared identity solution, each organization can access the data that is necessary and relevant for the provision of its services. This scenario would entail both authentication and identification. Interoperability between the various bodies and organizations involved could prove beneficial, with the system acting as a single gateway for

humanitarian assistance. This would entail applying the “once-only” principle²⁴² in humanitarian action to facilitate the provision of physical or digital services directly to beneficiaries through online platforms and/or the exchange of information or documents (automatically or on request) between various Humanitarian Organizations.²⁴³ Yet organizations will need to consider a range of factors when opting for such solutions. For example, they should identify the applicable governance framework and ensure that the roles played by those involved in the system (Data Controllers and Data Processors) are clear. Since appropriately segregating access to data can be technically difficult, it is not uncommon for Data Breaches to occur in unified commercial solutions. Likewise, in a unified system, the complex relationships between organizations can make it hard to ensure that data is only used for the purposes for it was collected. In addition, complex systems such as these can lead to the *de facto* exclusion of certain groups who may lack the requisite digital literacy skills.

Scenario 4: In some contexts, Humanitarian Organizations may issue functional identity documents to beneficiaries, such as registration cards allowing affected people to access their services. These may end up serving as foundational identity documents for authorities or financial institutions that accept them as proof of ID.

EXAMPLE:

In Jordan and Egypt, two countries that receive a large influx of refugees, local authorities require a valid passport or government-issued identification such as a Jordanian Ministry of Interior service card for refugees and asylum seekers to meet mobile SIM registration and Know Your Customer (KYC) requirements. UNHCR argues that its own identification documents should also be accepted, as these may be the only forms of ID that asylum seekers and refugees have.

12.1.5 DIGITAL IDENTITY AS FOUNDATIONAL IDENTITY

Various ongoing initiatives are aiming to develop Digital Identity systems that serve as a form of foundational identity for people without ID documents.

These initiatives are inspired by the fact that people who cannot prove who they are find it harder to assert their rights, access public services, and claim benefits and entitlements based upon their age, nationality, circumstances or any other identity

²⁴² The once-only principle implies that individuals provide their personal information to the authorities only once and that afterwards, at their request or with their consent, government departments may exchange the information for the fulfilment of their public duties instead of collecting it again.

²⁴³ See: European Data Protection Supervisor (EDPS), *Opinion 8/2017: EDPS Opinion on the proposal for a Regulation establishing a single digital gateway and the ‘once-only’ principle*, EDPS, 1 August 2017: https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdf.

and status attributes.²⁴⁴ Since proof of ID has become a prerequisite for accessing many services, the identity gap is a major barrier to participation in political, social and economic life. For example, private service providers often require a proof of ID to comply with legal requirements or as part of their due diligence processes (such as KYC, prevention of fraud and impersonation, and transaction risk and cost reduction). Digital Identity systems could be one way to help people in need but who lack identity documents. As mentioned above, however, very few Humanitarian Organizations have the mandate – and therefore the legitimate basis – to develop and deploy foundational systems of this type.

Importantly, Digital Identity programmes are not limited to specific technologies or systems. Such programmes can be designed using one of many technologies, or a combination of solutions. Technologies frequently associated with Digital Identity include:

- **Biometrics:**²⁴⁵ Enrolling beneficiaries in Digital Identity schemes in the humanitarian sector may include the use of biometrics such as fingerprints or iris scans.
- **Blockchain:**²⁴⁶ Blockchain is one possible way for individuals with limited access to digital technology and infrastructure to prove their identity.²⁴⁷ Despite its promise, however, the challenges that come with Blockchain technology demand serious consideration.
- **Data Analytics:**²⁴⁸ Digital Identities can be created from digital behavioural attributes (also called algorithmic ID) without using official credentials. Here, a person's online activity (social media use, browsing history, online purchases, call history, etc.) could be used to verify their identity.²⁴⁹ Although the potential of profile-based identity systems is not yet fully realized, this approach does raise data protection concerns.²⁵⁰

²⁴⁴ G. Verdirame et al., *Rights in Exile: Janus-Faced Humanitarianism*, Berghahn Books, New York, 2005, pp. 59–63.

²⁴⁵ See [Chapter 8: Biometrics](#).

²⁴⁶ See [Chapter 14: Blockchain](#).

²⁴⁷ A. Beduschi et al., *Building Digital Identities: The challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems*, University of Exeter and Coalition, 2017, pp. 15–16, p. 26: https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf.

²⁴⁸ See [Chapter 6: Data Analytics and Big Data](#) for issues related to the use of Data Analytics.

²⁴⁹ A. Beduschi et al., 2017, p. 8.

²⁵⁰ E.g. Facebook shadow accounts. See: R. Brandom, “Shadow profiles are the biggest flaw in Facebook's privacy defense”, 11 April 2018: <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>.

12.2 DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) involves identifying, evaluating and addressing the impacts on Data Subjects and their Personal Data of a project, policy, programme or other initiative that entails the Processing of such data. It should ultimately lead to measures that minimize the risks to the rights and freedoms of individuals and should follow a project or initiative throughout its lifecycle. In light of the large-scale Processing that Digital Identity systems involve, and of other potential risks and harm to Data Subjects arising from their use, Humanitarian Organizations should carry out a DPIA both before and during system and programme implementation. In addition, the DPIA process should analyse not just compliance with data protection requirements, but also the potential adverse impacts of the system on a variety of fundamental rights, as well as the ethical and social consequences of the data Processing.²⁵¹

The use of identity systems for multiple humanitarian purposes – some of which are not always identified from the outset – poses the risk of so-called function creep. This occurs when Humanitarian Organizations – intentionally or otherwise – misuse beneficiaries' data by using the identity system for purposes that were not originally foreseen. Moreover, governments and non-State armed groups that do not respect human rights could access identification and other systems to identify enemies or opponents, or to target and profile certain groups based on their ethnicity, political opinion, nationality or other characteristics. This information can then be used to control, discriminate and harm these individuals or groups in different ways, for instance by excluding them from essential services and aid, depriving them of their liberty and their right to a fair trial, or even committing atrocities (such as the Rwandan genocide and persecution in Nazi Germany, where identification and profiling played an essential role).

12.3 DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default is a practice that should feature throughout the lifecycle of applications that process Personal Data.²⁵² It involves designing a Processing operation, program or solution in a way that implements key data protection principles from the outset, and that provides the Data Subject with the greatest possible data protections. The key data protection principles in this sense are:

²⁵¹ A. Mantelero, “AI and Big Data: A blueprint for a human rights, social and ethical impact assessment”, *Computer Law & Security Review*, Vol. 24, Issue 4, August 2018, pp. 754–772, p. 755: <https://doi.org/10.1016/j.clsr.2018.05.017>.

²⁵² L. Jasmontaite *et al.*, “Data Protection by Design and by Default: Framing Guiding principles into Legal Obligations in the GDPR”, *European Data Protection Law Review*, Vol. 4, Issue 2, 2018: <https://edpl.lexxion.eu/article/EDPL/2018/2/o>.

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation (limited retention)
- integrity and confidentiality (security)
- accountability.

When designing an identity system, Humanitarian Organizations should therefore start by considering their needs, then examining whether an identity system is necessary and proportionate to solve the identified problem. If an organization determines that it does require an identity system, it should think carefully about which type of system best fits its needs and is appropriate in the particular circumstances. Following this process will help the organization apply the principles of data minimization and proportionality, as explained in section 6 below.

Data protection by design also requires an organization to conceive systems in a way that makes it possible, and easier, for Data Subject to exercise rights (see section 5 below). For example, in a Digital Identity system, Data Subjects should, by default, have access to information notices, to all information linked to their identity, and to logs detailing who has accessed their data and for what purposes.

12.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

Digital Identity systems can involve a wide range of bodies and entities, including Humanitarian Organizations, governments, and commercial entities such as banks, payment system providers, IT network providers and biometrics companies. Consequently, it can be difficult to ascertain which parties should be treated as Data Controllers and Data Processors. Likewise, it can be hard to determine where the boundaries of responsibility and liability lie among the parties. To counter this problem, a Digital Identity system must be designed in a way that clarifies who the stakeholders are, what responsibilities and obligations they have, and what data categories and flows each one uses and for what purposes. When a Humanitarian Organization determines the means and purposes of the identification programme, it will act as the Data Controller and, therefore, will be potentially liable for breaches, misuse and other types of harm that may arise from the programme. In situations where joint controllership is established, or where a Data Processor processes Personal Data only on behalf of the Data Controller, it is best practice to allocate responsibilities among the parties in a written agreement.

12.5 RIGHTS OF DATA SUBJECTS

The possibility of developing Digital Identity systems that are controlled by the Data Subject is currently being explored through various initiatives. Such systems aim to shift control to individuals by allowing them to store identity data on their own devices without relying on a central repository and, when necessary, providing credentials to those who need to verify them.²⁵³ As discussed above, this could be achieved, for example, by building a system in which beneficiaries store their personal information on their own devices or in another storage medium of their choosing, and are able to decide when to share it with bodies and organizations involved in the humanitarian response. Some initiatives functional or foundational identity initiatives also aim to shift control to individuals, again by allowing them to store their Personal Data on their own devices and sharing it with others if and when they wish. Whether a control shift would actually happen in practice, however, is still matter of dispute. When pursuing such initiatives, it is important to ensure that individuals are aware of their rights and the risks of having this information stored on their personal devices, and that they are sufficiently equipped to be able to use such tools safely.

EXAMPLE:

The ID2020 Alliance was set up to influence the development of so-called “good” Digital Identities, under which individuals have full control of their identity and can determine what data is shared and with whom. According to the Alliance, “Today, most personal data is stored in silos. The more siloed and numerous your data becomes the less control you have over it.” To solve this, the Alliance proposes that individuals “must have control over their own digital identities, including how personal data is collected, used, and shared.”²⁵⁴

While such initiatives are not yet commonplace, Humanitarian Organizations can give beneficiaries more control over and access to their data by providing them with a login to access all information relating to their identity credentials and, if applicable, a personal profile created by the organization in question. The potential benefits and risks associated with this solution still need to be fully explored, so as to determine whether it works in practice and whether it genuinely shifts control to individuals. In theory, however, such a system could automatically inform beneficiaries of any third parties that have accessed their data, and whenever a Processing activity starts. It could also allow beneficiaries to update their Consent, when this is the legal basis for Processing, and to receive updated information about

²⁵³ M. Pisa and M. Juden, *Blockchain and Economic Development: Hype vs. Reality*, Center for Global Development, Washington, D.C., 2017, p. 25: https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_o.pdf.

²⁵⁴ All quotes from the ID2020 website: <https://id2020.org>.

the Processing. With more control, beneficiaries could directly exercise their rights as Data Subjects through an online profile or platform. In cases where beneficiaries are not digitally literate, or do not have access to the necessary technology, Humanitarian Organizations must provide alternative ways for them to exercise their rights in respect of their Personal Data.

12.5.1 RIGHT OF ACCESS

Beneficiaries have the right to request access to information about the Processing of their data, and to the data that are being processed.²⁵⁵ While this right can be limited in certain circumstances, Humanitarian Organizations, as Data Controllers, should reply to such requests by informing beneficiaries if their Personal Data are being processed and, if so, granting them access to the data in question. In practice, however, this right may be hard to implement in Digital Identity programmes as it can be difficult to verify that the person requesting access to information is the individual entitled to receive it (verification), particularly if the request is made by digital means (which is the most likely scenario in the case of Digital Identity). While this is an issue that applies to a wide range of digital systems, it must be given equal consideration in the case of Digital Identity. Humanitarian Organizations should therefore take steps to ensure that the rights of Data Subjects can be respected, both before deciding on the design of a Digital Identity system, and when deciding whether or not to implement it.

Another challenge to respecting the rights of Data Subjects in Digital Identity programmes stems from the fact that different units within the same organization might hold different pieces of information about the same Data Subject. Consequently, compiling all this information in order to respond to a request may prove challenging. It could even involve unnecessary effort, since beneficiaries often only request access to a specific category of data, or to data relating to a particular programme, as opposed to all the data about them that the organization holds. Organizations should therefore discuss this with the Data Subject, so as to understand the specifics of the request and avoid any superfluous effort. Humanitarian Organizations should factor this challenge into their thinking at the Digital Identity system design stage, so they can anticipate issues of this type and devise ways to prevent them. A login-based access system, such as the one envisaged above, could allow beneficiaries to access their profile at any time, check what information is held about them, and the purposes for which it is being used.

²⁵⁵ See [Section 2.11.2: Access](#).

12.5.2 RIGHTS TO RECTIFICATION AND ERASURE

Beneficiaries should be able to rectify incorrect data about themselves and, in certain circumstances, to have their data deleted. They could do this directly, for instance by logging into their account (as envisaged above). When beneficiaries do not have control over their data, exercising their rights can again prove challenging, not least when it comes to assessing and confirming the identity of someone requesting to have their data rectified or deleted. To address this problem, Humanitarian Organizations will need to implement a verification system that complies with the minimization principle and does not collect unnecessary Personal Data. Here again, having beneficiaries log into their account would be one way to achieve this aim.

12.6 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

While this section provides an overview of data protection concerns that may arise when dealing with Digital Identity systems, every case should be examined in detail and on its merits, taking into account the technology used and the type of identification needed to achieve the envisioned programme's objectives. Different programmes will have different requirements. Likewise, different technologies may have different Data Protection implications.

12.6.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations need to process Personal Data in order to establish or verify the identity of a beneficiary. These Processing operations may be carried out on one or more legal bases. Under scenarios 2 and 3, for instance, a Humanitarian Organization will have to identify a separate legal basis for each Processing activity, e.g. vital interest for the Processing of medical records, and Consent for the Processing of Personal Data for restoring family links.

On the issue of Consent, it is important to recognize that beneficiaries receiving aid may not be in a position to give it validly.²⁵⁶ Consent is a freely given, specific and informed indication that a Data Subject agrees to the Processing of their Personal Data. Similarly, while Humanitarian Organizations may use public interest as the legal basis for a programme that provides official identity credentials, failing to obtain Consent could lead to distrust among beneficiaries. They may feel that, because they have no say in the Processing of their Personal Data, their rights are being restricted. This is especially true when the data in question relate to their identity, which is an intrinsic part of a person's life.

²⁵⁶ See [Section 3.2: Consent](#).

12.6.2 PURPOSE LIMITATION AND FURTHER PROCESSING

Personal Data should be collected for specified, explicit and legitimate purposes, and further Processing should only be undertaken when compatible with the initial purposes.²⁵⁷ In this regard, it is important to consider whether Personal Data collected from a Data Subject in order to provide them with Digital Identity credentials under a specific humanitarian programme (e.g. with the aim of establishing beneficiaries' identity) could be further processed under a different programme (e.g. to provide assistance or services). Humanitarian Organizations should consider the following factors when applying the purpose limitation principle:²⁵⁸

- compatibility between the initial and further purposes
- the context in which the data are collected, including the relationship between the individual and the controller
- the nature of the data
- potential consequences for beneficiaries
- relevant safeguards (including data security safeguards, such as encryption or pseudonymization).

As Digital Identity systems can have multiple uses, each with its own purpose, organizations must clearly specify all the purposes of a given Processing operation. If these purposes change or are subsequently clarified, the organization will need to give further notice to the Data Subjects.

12.6.3 PROPORTIONALITY

The principle of proportionality calls for the least intrusive means of Processing to be used in achieving the specified Processing aims. It is worth recalling that some humanitarian activities, such as the provision of aid, may require beneficiaries to prove only that they are entitled to receive the benefit (i.e. authentication), while others will demand a foundational (or "official") identity (i.e. verification). For this reason, Humanitarian Organizations, as Data Controllers, should consider which activities require identification and which ones do not. By limiting the Processing to authenticating the entitlement of beneficiaries to access services, organizations could avoid accidentally or unintentionally repurposing data or gathering unnecessary information, since beneficiaries' legal identities would not be collected or stored by the organization in the first place. In cases where authentication or identification is needed, organizations should also consider how much data they require, and of what type. For example, when using biometric data, organizations should process the least data points possible (e.g. one fingerprint instead of ten).

²⁵⁷ See [Chapter 2: Basic principles of data protection](#).

²⁵⁸ EDPS, 2017, pp. 9–10.

12.6.4 DATA MINIMIZATION

Humanitarian Organizations should only collect and process the minimum amount of data they need to fulfil the purpose of the Processing. For that reason, they must fully understand what information they need from beneficiaries before implementing any identification system that processes Personal Data. If an organization establishes that proving entitlement only is sufficient (i.e. authentication), it should not collect or process identity information in any way.

12.6.5 DATA SECURITY

Digital Identity systems such as the one envisaged in scenario 3 could allow beneficiaries to store their Personal Data on their own devices. The same applies to initiatives designed to provide an identity to those who lack identity documents. In such cases, malicious individuals or organizations would, in theory, only be able to access this information if they were able to breach device security. Yet beneficiaries could also be physically coerced into handing over their devices.

In other cases, such as the ones mentioned in scenarios 1 and 2, Humanitarian Organizations may store Personal Data in their own databases as part of a Digital Identity programme. These databases could become a target for malicious individuals or organizations. Consequently, Humanitarian Organizations must ensure that their Digital Identity systems preserve the confidentiality, availability and integrity of data in their systems and, in doing so, adequately protect the data from misuse, data breaches and liabilities.²⁵⁹ Furthermore, the sensitive nature of certain types of Personal Data will generally require a very high level of security. Encryption techniques such as secret sharing (also known as secret splitting) systems can help increase security. In such systems, data are encrypted and the key is fragmented between multiple parties, which then need to work together to decrypt the data (e.g. different Humanitarian Organizations, as envisaged in scenario 3), thereby avoiding a single point of failure. Under this arrangement, the key can easily be destroyed if needed, since deleting a certain number of fragments (the number varies from system to system) would mean the data could no longer be used.

When implementing identity programmes, Humanitarian Organizations should also consider the security measures adopted by any partners. For instance, if beneficiaries' information is shared with other bodies or organizations, they must have appropriate security measures in place to protect the data and avoid the harmful consequences of a data breach.

²⁵⁹ USAID, 2017, p. 25.

12.6.6 DATA RETENTION

Personal Data should be retained for a defined period, which should be no longer than is necessary for the purpose of the Processing. Where the main purpose of the Processing is to provide basic humanitarian assistance in the form of food, shelter and medical care, Personal Data should only be retained for as long as is needed to provide that assistance. Yet for the situation is more complicated for Digital Identity programmes that seek to provide a form of identity credentials for beneficiaries who lack identity documents, since beneficiaries may wish to continue using their identity – which replaces or serves as an identity document – throughout their entire lives, as well as updating their status or situation as time passes. Here, determining an appropriate data retention period can prove challenging. Humanitarian Organizations should, however, provide an initial indication of the retention period that is consistent with the initial purpose for which the data are being collected. Once this period ends, organizations involved in programmes of this type should conduct periodic assessments to determine whether they still need to retain the data. Another option would be to allow beneficiaries to decide whether their data can be retained.

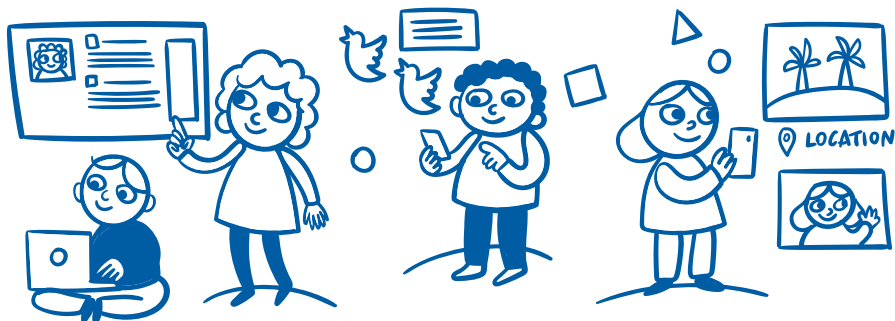
12.7 INTERNATIONAL DATA SHARING

Depending on the technical solution and the design chosen, data processed in Digital Identity systems may routinely flow across national borders. In scenario 3 above, for instance, multiple organizations may share information with each other, or beneficiaries may share their data with multiple organizations simultaneously. International data sharing raises data protection concerns.²⁶⁰ Although some jurisdictions have recognized protection arrangements (such as the use of contractual clauses), Humanitarian Organizations operating Digital Identity programmes may struggle to implement these arrangements in practice because the system may involve multiple parties in different locations. As a general rule, Humanitarian Organizations are advised to take whatever steps they can to ensure that any transfer of Personal Data to a third party (and any subsequent onward transfer) does not lower the level of protection of individuals' rights. Because organizations are liable for all data transfers they conduct, they are responsible if data is unlawfully shared with other organizations in the envisaged scenario. Beneficiaries' Consent, however, could be an appropriate legal basis for organizations to transfer data in some situations. As mentioned above, however, it is questionable whether beneficiaries receiving aid can always give valid Consent.²⁶¹ In such cases, a different legal basis will have to be identified.

²⁶⁰ See [Chapter 4: International Data Sharing](#).

²⁶¹ See [Section 3.2: Consent](#).

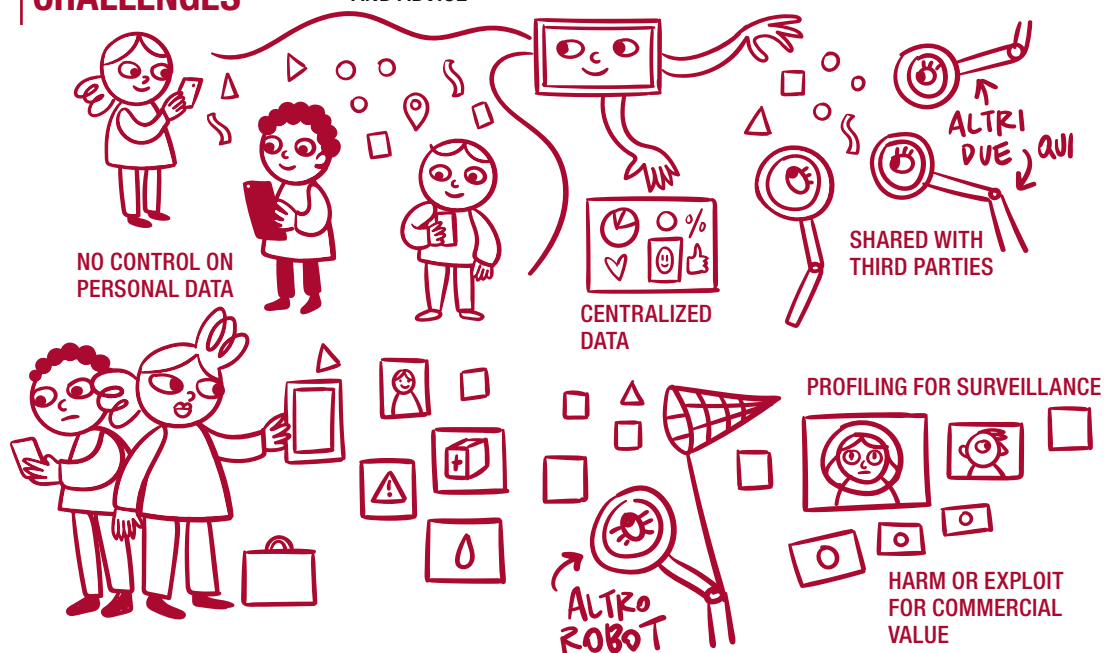
SOCIAL MEDIA



POSSIBLE USE



CHALLENGES



CHAPTER 13

SOCIAL MEDIA^{262,263}

262 This chapter focuses on the use of social media by Humanitarian Organizations to communicate and engage with beneficiaries. For information related to the use of social media to identify crises and improve the humanitarian response, please refer to [Chapter 6: Data Analytics and Big Data](#). For messaging apps, please refer to [Chapter 11: Mobile Messaging Apps](#).

263 The editors would like to thank Nicolas de Bouville (Facebook), Camila Graham Wood, Antonella Napolitano, Ed Geraghty (Privacy International) for their contributions to this chapter.

13.1 INTRODUCTION

13.1.1 SOCIAL MEDIA IN THE HUMANITARIAN SECTOR

Humanitarian Organizations interact with beneficiaries via social media in a variety of ways. In emergencies, for instance, they may use social media to inform people about safe places and the delivery of aid. They may also use social media to raise awareness (such as addressing humanitarian needs arising in the framework of migration), to encourage beneficiaries to share information with each other in an emergency, or to provide information about health and medical care.

Engaging with beneficiaries in this way carries a number of risks. When individuals view or reply to public or private social media posts by Humanitarian Organizations, or when they join public or private groups hosted by such organizations, they share a rich variety of data with the platform in question. Both Humanitarian Organizations and beneficiaries may engage with each other on social media without necessarily being fully aware that they are generating both data and metadata (a set of data that describes and gives information about other data)²⁶⁴ that can be collected by social media platforms, then used to profile an individual to determine characteristics such as key aspects of their identity, their networks, views and opinions, preferences and affiliations. Likewise, organizations and beneficiaries may be unaware of the consequences and risks of such Processing.

Although individuals may engage with Humanitarian Organizations informally, in a manner akin to a private conversation, the way social media platforms are designed and operate means that third parties may be able to monitor, collect, retain and analyse their exchanges. These third parties include not only social media providers, but also corporate entities, law enforcement agencies, immigration and border authorities, and governments, who use open-source intelligence techniques and sophisticated social media monitoring tools. Data, including images shared on social media, can be analysed in a range of ways – from image and facial recognition, to sentiment and emotion recognition²⁶⁵ – often using opaque algorithms and Machine Learning.²⁶⁶ This type of profiling adds to the opacity of how individuals can be exposed through their interactions with, and use of, social media. When decisions are made based on such profiling, it can have serious consequences for an individual, because this opacity brings added risks that come from unequal access

²⁶⁴ For more on metadata, see: ICRC and Privacy International, *The Humanitarian Metadata Problem: Doing no Harm in the Digital Era*, Privacy International and ICRC, 2018: <https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf>.

²⁶⁵ See, for example: F.M. Plaza-del-Arco *et al.*, “Improved emotion recognition in Spanish social media through incorporation of lexical knowledge”, 27 September 2019: <https://www.sciencedirect.com/science/article/pii/S0167739X1931163X>.

²⁶⁶ See [Chapter 16: Artificial Intelligence and Machine Learning](#).

to data and to justice, such as the inability to challenge incorrect assumptions that influence or determine decision-making processes and outcomes.

While social media can help Humanitarian Organizations provide services, using these platforms can cause organizations to lose control of the data generated and shared, and pose medium- or longer-term risks. These must be assessed through clear procedures and risk assessments (see Section 2 on Data Protection Impact Assessments below).

Below are some examples of cases where Humanitarian Organizations have used social media to engage with beneficiaries:²⁶⁷

- Facilitating emergency management by contributing to the mitigation, preparedness, response, and recovery of disasters and emergency situations:** In Bangladesh, the creation of a national coordination platform allowed Humanitarian Organizations, in coordination with the government, to broadcast easily understandable disaster-preparedness messages through social media during emergencies to facilitate the disaster preparedness stage of emergencies.
- Improving the quality of aid delivery:** In 2016, the ICRC doubled the amount of food contained in food parcels delivered in Syria, as the security situation led to longer periods between food distribution. Beneficiaries were informed of this change in a short video shared on ICRC's institutional Facebook page. Through the comments feature, beneficiaries also had the opportunity to reply to the video and explain their needs (e.g. requesting better cardboard boxes so the food inside would not be damaged in transit). The ICRC then replied to the comments, explaining what it was doing to fulfil the requests or why it could not do so.
- Improving the efficiency of services:** The Kenyan Red Cross Society (KRCS) actively monitors social media platforms to find out about road accidents and dispatch ambulances to those locations. Knowing this, Kenyans frequently flag road-traffic accidents to the KRCS through social media.
- "Information as aid" and health promotion:** MSF and other NGOs use social media to provide health information and advice to beneficiaries.

Although social media platforms offer a wide range of opportunities, using them can also pose risks to beneficiaries and raise important responsibility questions for Humanitarian Organizations. This chapter will discuss how data are generated on social media before addressing core data protection concerns.

²⁶⁷ Examples taken from: T. Lüge, *How to Use Social Media to Better Engage People Affected by Crises: A brief guide for those using social media in humanitarian organizations*, ICRC, IFRC and UN-OCHA, 2017: <https://www.icrc.org/en/document/social-media-to-engage-with-affected-people>.

13.1.2 SOCIAL MEDIA AND DATA

13.1.2.1 What data are generated on social media and how?

Social media platforms receive, capture, generate and process large amounts of data from users, including metadata, user location, images, contacts, “likes”, and attention and interest indicators, using them for various purposes. Even when users explicitly enquire about their data, there is often little transparency as to what specific data are being created, and how the platform and other third parties are accessing and using these data for profiling and other purposes.

Some of the data collected by social media platforms come directly from the individual (this is known as “declared data”), such as when they sign up for an account (a name or username, sometimes a copy of an identity document, a phone number, an email address and a physical address), or when they post photographs or comments on their profile.²⁶⁸

Social media platforms also process so-called “inferred data” – additional data not provided directly by users themselves but inferred from their declared data. Here, the declared data includes both data provided directly by the user, and data about the user coming from other apps or platforms, which sometimes automatically transfer Personal Data to social media platforms when a user opens the app or accesses its services, even before obtaining Consent.²⁶⁹ This happens, for example, when an online store notifies a social media platform that a user has accessed their website so that the platform can use their shopping preferences to offer them targeted advertisements.

Social media platforms usually combine data obtained from different sources and, applying Data Analytics,²⁷⁰ create a user profile that monitors the user’s activities and behaviour.²⁷¹ For example, providers can infer who someone’s friends are from how often then communicate and interact on social media.²⁷² Understanding someone’s routine and behaviour allows platforms to offer targeted services and individualized content to their users.²⁷³

²⁶⁸ ICRC and Privacy International, 2018, p. 34.

²⁶⁹ Privacy International, “Investigating Apps interactions with Facebook on Android”, 2019: <https://privacyinternational.org/appdata>.

²⁷⁰ See [Chapter 6: Data Analytics and Big Data](#).

²⁷¹ EU Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 2018, p. 12.

²⁷² ICRC and Privacy International, 2018, p. 35.

²⁷³ For more on target advertising, see: Privacy International, “AdTech”: <https://privacyinternational.org/topics/adtech>.

Evidence shows that it is possible to build a profile-type identity from someone's digital behavioural attributes, i.e. their online activity.²⁷⁴ Consequently, a person's digital traces can be used to create a digital profile even without their knowledge²⁷⁵ and infer information about them including their gender, sexual orientation, religion, location, interpersonal relationships and anticipated behaviour.²⁷⁶ This type of profile is then used for targeted advertising, but has also been used in the past for political campaigning, as well as predictive policing.²⁷⁷ This means that if Humanitarian Organizations encourage beneficiaries engage with them on social media, they may be facilitating this kind of targeting.

Examples of data that may be collected:

Facebook divides the data it collects into various categories: data a user provides, data provided by other users about a user, data about users' networks and connections, payment information and device information, and information from partners such as advertisers, app developers and publishers.²⁷⁸ Under each category, there is a long list of data that the platform collects, including:

communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created.²⁷⁹

The list also includes "information about operations and behaviours performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements"²⁸⁰ as well as Bluetooth signals, and information about nearby Wi-Fi access points, beacons and cell towers.

Twitter, in turn, collects data related to a user's basic information (such as declared name, username and email address), profile information, contact information and public information (tweets as well as metadata generated by tweets such as time and location).²⁸¹

²⁷⁴ A. Beduschi *et al.*, "Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for new Digital Identity Systems", *Open Research Exeter*, 2017, p. 8: <https://ore.exeter.ac.uk/repository/handle/10871/28297>.

²⁷⁵ E.g. Facebook shadow accounts. See: <https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy>.

²⁷⁶ ICRC and Privacy International, 2018, p. 90.

²⁷⁷ See, for example: A. Meijer and M. Wessels, "Predictive Policing: Review of Benefits and Drawbacks", *International Journal of Public Administration*, Vol. 42, Issue 12, 2019, pp. 1031–1039, DOI: 10.1080/01900692.2019.1575664. Predictive policing is considered to be part of law enforcement practices.

²⁷⁸ Facebook data policy: https://www.facebook.com/full_data_use_policy.

²⁷⁹ Facebook data policy.

²⁸⁰ Facebook data policy.

²⁸¹ ICRC and Privacy International, 2018, p. 96.

13.1.2.2 What data can be shared with third parties?

Some social media platforms may share the information they collect with other service providers for purposes such as targeted advertising of individuals with specific profiles. Given the exponential growth of social media platforms, the number of people and advertising companies that have access to personal information has vastly increased in recent years, thereby increasing the possibility that individuals could be tracked through different methods. Moreover, social media platforms receive data from other parties and organizations through partnership arrangements, and these additional data are used to further develop a user's profile for various purposes, including advertising.

Examples of how social media data may be shared:

Facebook shares aggregated information it collects from users and non-users of the network with other Facebook companies (including Instagram, WhatsApp and Messenger) and third-party partners. It also allows users to share data they store on Facebook with third-party apps, websites or other services that use or are integrated with Facebook.²⁸² This means that users may (knowingly or otherwise) share data that is not related solely to them, such as their friends list. Consequently, “even when a user ‘locks down’ their profile, their data could still be collected by a third-party app being used by one of their friends”.²⁸³

Facebook also offers a variety of options for advertisers to benefit from users' profiles. For instance, advertisers may upload an email or phone list of registered customers and ask Facebook to find their social media profiles in order to target them for marketing purposes (known as a “custom audience”).²⁸⁴ This way, advertisers benefit from aggregated information provided by Facebook, while the social media platform also gathers data from the advertiser. Companies may also ask Facebook to find profiles that are similar to existing customers in order to increase their range of advertising, to focus on specific locations, demographics or genders, or even to install pixels²⁸⁵ on their websites, so that when a Facebook user visits their website, they receive ads from the company on their Facebook page.²⁸⁶ Since December 2019, however, Facebook no longer allows phone numbers provided by users when signing up for two-factor authentication to be used to make friend

²⁸² Facebook data policy.

²⁸³ ICRC and Privacy International, 2018, p. 96.

²⁸⁴ Facebook, “About Custom Audiences from customer lists”: <https://www.facebook.com/business/help/341425252616329>.

²⁸⁵ Facebook pixel is a Facebook analytics tool that allows businesses to better target their advertisements by measuring their effectiveness and understanding the actions people take when visiting the business' website. See: “About Facebook Pixel”: https://www.facebook.com/business/help/742478679120153?helpref=page_content.

²⁸⁶ B.V. Alsenoy et al., *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms*, Belgian Privacy Commission, 2015, pp. 55–64.

suggestions.²⁸⁷ This change in company practice reflects increased recognition of the implications of data-sharing between platforms and third parties. This is further demonstrated by the new Off-Facebook Activity tool,²⁸⁸ which allows users to segregate information obtained by third parties from their Facebook profile.

Twitter, in turn, allows users to opt out of much of its Processing activities. By default, however, everything shared and published on the platform is public unless the user specifies otherwise. In practice, this means Twitter:

is allowed to share or disclose a user's public information (such as profile information, public tweets, or followers) to a wide range of users, services and organizations. Twitter further maintains the right to infer, from these data, which topics might be of interest to the user.²⁸⁹

13.1.2.3 What data can law enforcement and government authorities obtain?

National law may require social media platforms to store users' Personal Data so that public authorities can access it to identify an individual or obtain information about their online activity for law enforcement purposes.²⁹⁰ In some – but not all – jurisdictions, a warrant may be needed to access such information.

While there may be some publicly available information on government access requests, particularly in jurisdictions with a judicial process, only a few social media companies publish transparency reports.²⁹¹

Using various tools, including those provided by the platforms themselves (the so-called “firehose”), law enforcement agencies and other third parties can directly access social media through what is known as open-source intelligence (OSINT), i.e. intelligence gathered from publicly available data. They can also use social media intelligence (SOCMINT), which involves monitoring and gathering both publicly available and private information on social media platforms.²⁹² These practices are unregulated in many jurisdictions, and the law is often unclear as to whether such monitoring is legal. Further invasive techniques also enable data and information

²⁸⁷ K. Paul, “Facebook separates security tool from friend suggestions, citing privacy overhaul”, Reuters, 19 December 2019: <https://www.reuters.com/article/us-facebook-privacy-idUSKBN1YN26Q>.

²⁸⁸ Facebook, “Now You Can See and Control the Data That Apps and Websites Share with Facebook”, 20 August 2019: <https://about.fb.com/news/2019/08/off-facebook-activity/>.

²⁸⁹ ICRC and Privacy International, 2018, p. 97.

²⁹⁰ ICRC and Privacy International, 2018, p. 34.

²⁹¹ Facebook, “Government Requests for User Data,” 2018: <https://transparency.facebook.com/government-data-requests>; Twitter, “Twitter Transparency Report”, 2018: <https://transparency.twitter.com/en.html>.

²⁹² Privacy International, “Social Media Intelligence”: <https://privacyinternational.org/explainer/55/social-media-intelligence>.

physically stored on a device²⁹³ or in cloud-based applications²⁹⁴ to be extracted. As with SOCMINT, mobile phone and cloud extraction technologies are used with little transparency and remain unregulated in a number of jurisdictions. In practice, as social media storage is often cloud-based, the volume of Personal Data that can be obtained through these methods is very large.

13.2 DATA PROTECTION IMPACT ASSESSMENTS

Humanitarian Organizations cannot fully control how social media platforms operate, or how they generate and process data. But they can – and should – conduct risk assessments to understand the consequences of using social media to interact with beneficiaries before deciding whether to use such platforms, how to use them and for what purpose.

Humanitarian Organizations use social media with the expectation that beneficiaries have already signed up and consented or otherwise agreed to the platform's terms and conditions. This expectation does not relieve organizations of their duty to carry out a Data Protection Impact Assessment (DPIA).²⁹⁵ The purpose of a DPIA is to identify how social media use will affect beneficiaries, and measures the organization can take to mitigate potential risks. In particular, a DPIA should not only look at data protection risks, but also evaluate whether social media use in a particular context could lead to human rights violations or otherwise harm the individuals in question. These risks should then be weighed against the potential benefits.

It is worth stressing again that, aside from the content users generate and provide when they sign up for their account(s), the use of social media also generates a large amount of data and metadata that platforms do not pro-actively declare. Consequently, users may not even be aware these data are being generated and processed.²⁹⁶ For example, merely clicking “like” buttons or links that redirect the user to other websites generates metadata.

293 See, for example: Privacy International, “Push This Button For Evidence: Digital Forensics”: <https://privacyinternational.org/explainer/3022/push-button-evidence-digital-forensics>; and Privacy International, “Can the police limit what they extract from your phone?”, 14 November 2019: <https://privacyinternational.org/node/3281>.

294 Privacy International, “Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps”, 7 January 2020: <https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data>.

295 See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

296 ICRC and Privacy International, 2018, p. 17.

In recent years, many governments have gained access to, and made use of, large amounts of social media data and metadata, as well as to powerful analysis tools that help them identify patterns in such data and profile individuals and groups.²⁹⁷ The DPIA must therefore go beyond merely analysing compliance with data protection requirements. It should also address how the use of a certain application or platform could positively or negatively impact a variety of fundamental rights, as well as the ethical and social implications of Processing by Humanitarian Organizations.²⁹⁸

The Processing of metadata can carry significant risks. In 2014, for instance, a former director of the U.S. National Security Agency (NSA) said that they would take the decision to kill people based on information acquired via metadata.²⁹⁹ Fintech and advertising companies are also employing numerous techniques to make use of such data.³⁰⁰ That is why it is important for Humanitarian Organizations to take the non-humanitarian purposes and consequences of using social media into account when conducting a DPIA and developing their social media use strategy.

Likewise, the DPIA should consider the fact that social media providers' business models rely on monetizing user data (e.g. for ad targeting). This means that data gathered for humanitarian purposes through such platforms might be vulnerable to commercial exploitation and surveillance.

Humanitarian Organizations should also assess whether social media platforms are the safest and most reliable way to communicate with beneficiaries. In emergencies, for example, governments can shut down social media to avoid the spread of fear or false information,³⁰¹ meaning Humanitarian Organizations will need to consider alternative means of communication.

²⁹⁷ ICRC and Privacy International, 2018, p. 29.

²⁹⁸ A. Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", *Computer Law & Security Review*, Vol. 34, Issue 4, 2018, pp. 754–772: <https://doi.org/10.1016/j.clsr.2018.05.017>.

²⁹⁹ ICRC and Privacy International, 2018, p. 22.

³⁰⁰ ICRC and Privacy International, 2018, pp. 23–24.

³⁰¹ See, for example: J. Wakefield, "Sri Lanka attacks: The ban on social media", BBC, 23 April 2019: <https://www.bbc.com/news/technology-48022530>.

13.3 ETHICAL ISSUES AND OTHER CHALLENGES

For Humanitarian Organizations, involving social media platforms in their work inevitably raises ethical issues because the organization does not have control over third parties' privacy and data protection policies. Many of these platforms rely on exploiting and monetizing users' data³⁰² – both declared data and inferred data, which can reveal sensitive information such as a person's sexual orientation, religion, political opinion and ethnicity.³⁰³ By engaging with beneficiaries on social media, Humanitarian Organizations contribute to the generation of the data and metadata from which these inferences are made.³⁰⁴

Likewise, social media platforms change their terms and conditions, privacy policies and Processing activities all the time, without always requesting users' Consent. In addition, although users may understand that the platform processes declared data, platforms may not be transparent about what they infer from such data – and, more importantly, from information obtained from other sources (such as online activity, other users and third parties), as well as from data generated by design and default because of the way the platform is designed and operates.³⁰⁵ The information gathered – and, ultimately, the decisions made on the basis of this data – can severely and adversely affect a user's life, as the example below shows:

Social media data are being increasingly used to assess the credibility of users requesting loans and to monitor those who have already been given a loan. These assessments are based on a selection of indicators that categorize people as either a “reliable, trustworthy borrower” or an “unreliable, risky borrower”.³⁰⁶

Aside from the risks associated with the sharing of data by beneficiaries on social media platforms, Humanitarian Organizations must also be mindful about the content they themselves share. Some content, such as public photographs or videos including beneficiaries, can have negative consequences for the individuals in question, from profiling and targeting by companies, to persecution, intimidation and blackmail, discrimination, identity theft, and loss of control over their data.

³⁰² See, for example: Privacy International, “Guess what? Facebook still tracks you on Android apps (even if you don't have a Facebook account)”, 5 March 2019: <https://privacyinternational.org/blog/2758/appdata-update>; and Privacy International, *How Apps on Android Share Data with Facebook – Report*, Privacy International, 2018: <https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report>.

³⁰³ ICRC and Privacy International, 2018, pp. 89–90: <https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report>.

³⁰⁴ ICRC and Privacy International, 2018, p. 91.

³⁰⁵ ICRC and Privacy International, 2018, p. 102.

³⁰⁶ ICRC and Privacy International, 2018, p. 106. See also: Privacy International, “Fintech”: <https://privacyinternational.org/topics/fintech>.

Organizations should also remember that social media may not always be the most useful or effective way to reach a given audience. Social media use is often limited in rural and remote areas, and not all members of a target population may have equal access to technology. Likewise, in some contexts, most social media users will be male, so using platforms for women's health initiatives is unlikely to be effective.

13.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

When Humanitarian Organizations use social media for communication purposes, their role in relation to the Processing of beneficiaries' Personal Data is often not entirely clear. When organizations set up an institutional page or profile on a social media platform, for instance, the platform's terms and conditions might allow the provider to process more data through that page, or to profile users for advertising purposes. Here, the organization could arguably be considered a joint controller with the platform, and therefore bears part of the responsibility for the Processing. However, when an organization simply uses the platform to interact with beneficiaries through a page, profile or group created by beneficiaries themselves, it is harder to establish the organization's role and the extent of its responsibility.

Example of joint controllership:

In 2018, the Court of Justice of the European Union (CJEU) ruled, in case C-210/16, that administrators of Facebook pages are Data Controllers in relation to the Personal Data collected and processed by Facebook through their fan pages (a fan page is an institutional page, created by the company or organization on the Facebook platform, to communicate with Facebook users and share content about their work).³⁰⁷ As fan pages are hosted on the Facebook platform, Facebook gathers information about those who access or interact with it, regardless of whether they have platform Facebook account. Facebook uses this information to produce statistics about fan page visitors, which are shared with the page's administrator.

According to the Court, the administrators of such pages (i.e. the organizations that create and manage them) are Data Controllers because creating the fan page "gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account" (para. 35). Furthermore, where administrators define specific parameters to be collected by Facebook to benefit from statistics about the page's visitors, they are considered to be taking part in the determination of the means and purposes of the Processing.

³⁰⁷ Court of Justice of the European Union (CJEU), Case 210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Judgement ECLI:EU:C:2018:3885, June 2018.

Although this ruling relates to the European Union regulatory context and only concerns Facebook, the influence of EU data protection law means that this broad (albeit controversial) definition of controllership may also be adopted in other regions. Should that be the case, Humanitarian Organizations might be considered Data Controllers in relation to the Processing of Personal Data by the social media platforms they use in relation to their page. In practice, this means that, where the platform processes Personal Data collected through the organization's page for non-humanitarian purposes, the organization in question could be responsible for such Processing.

Humanitarian Organizations must therefore do everything they can to fully understand the business models, privacy policies and security protocols of the social media platforms they use, since they could be held liable for misuses by the platform and other third parties. If there are any doubts regarding compliance with data protection, human rights and humanitarian principles, organizations should always choose a safer communication option.

13.5 BASIC DATA PROTECTION PRINCIPLES

13.5.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

While Humanitarian Organizations cannot control how social media platforms operate and process data, they should still determine the legal basis for Processing data that they may request and/or receive through social media. For instance, Humanitarian Organizations may sometimes use images of beneficiaries in public relations campaigns. Where Consent is relied upon, an individual must be able to withdraw Consent. Yet once an image or video is published online, the organization may lose control of its copies and reproductions and, should a beneficiary withdraw Consent, the organization may not be able to remove the content entirely.

Humanitarian Organizations must identify a legal basis for each Processing activity.³⁰⁸ Organizations frequently use the same social media page or profile both for their humanitarian work, and for campaigning and fundraising, which may make it difficult to differentiate each purpose in practice. In such cases, it is important to consider the purpose of each element of a Processing activity and to document it accordingly.³⁰⁹

³⁰⁸ See [Chapter 3: Legal bases for Personal Data Processing](#).

³⁰⁹ See [Chapter 3: Legal bases for Personal Data Processing](#).

13.5.2 INFORMATION

Individuals should be given clear and timely information regarding the Processing of their data by the Data Controller,³¹⁰ explaining what data are collected (in order to provide a service, for instance), what data are generated by the use of the service, what the purposes of the collection are, and who can access, share and/or use the individual's Personal Data. This information allows Data Subjects to make informed decisions about whether to use a specific service, and to understand how to exercise their rights. Yet when Humanitarian Organizations interact with beneficiaries through social media, the data are primarily generated and processed directly through the platforms themselves, leaving Humanitarian Organizations with little control over the actions mentioned above. Organizations should nevertheless take responsibility for providing relevant information as far as possible.

Again, it should be stressed that platforms regularly change and update their privacy and data protection policies, which can make it very difficult for users to understand what data are being generated and processed (i.e. how they are used and with whom they are shared).³¹¹ It is therefore challenging for Humanitarian Organizations to understand the risks that using social media platforms presents, and it is unclear what information organizations should provide to Data Subjects. Humanitarian Organizations are advised, at the very least, to inform beneficiaries about the Processing activities for which they are responsible – for instance, explaining why they are communicating through social media, and how the information beneficiaries share with the organization will be used and for what purposes.

Although Humanitarian Organizations have no control over what social media platforms do with the data they collect, some organizations have carried out online awareness-raising campaigns to explain the risks associated with social media and what actions beneficiaries should take to protect their data. In Mexico, for instance, UNHCR uses the El Jaguar page to communicate with beneficiaries. The organization produced a video, shared via the page, warning beneficiaries about the risks associated with using Facebook and how to minimize them.³¹²

Campaigns like these help beneficiaries understand the chain of parties and organizations that may have access to the data they produce on social media, and the risk of harm that might come from these platforms. Yet informing beneficiaries about social media data and privacy policies may not prove helpful if they cannot find an alternative to their current platform. Instead, Humanitarian Organizations should focus on informing beneficiaries about the potential and most likely risks

³¹⁰ See [Section 2.10: Information](#).

³¹¹ ICRC and Privacy International, 2018, p. 17.

³¹² See the campaign video (in Spanish) at: <https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680/>.

they will encounter when, for instance, they join their groups or follow their pages on social media, and on explaining whether membership of such communities may be visible to others or may be used against them in any way. This is particularly important since, data protection concerns aside, social media use poses other risks such as surveillance and consequent identification (and potential location) of vulnerable people and groups by ill-intentioned parties.

13.5.3 DATA RETENTION

According to the data retention principle, data should be retained for a defined period necessary for the purposes for which it was processed. This period can be three months, a year, the duration of a crisis, or some other time frame.³¹³ When it is not possible to determine the retention period at the time of collection, a review should be conducted at the end of an initial period.

When Humanitarian Organizations interact with beneficiaries through social media, the platforms themselves collect and retain their data. The retention period will therefore vary from one platform to the next.

Examples of Facebook's data retention policy:

Facebook's data policy stipulates that data are retained until they no longer necessary to provide the services or until the account is deleted, although there is evidence that the platform keeps some data even after deletion of the account.³¹⁴ The policy explains further:

This is a case-by-case determination that depends on things like the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when you search for something on Facebook, you can access and delete that query from within your search history at any time, but the log of that search is deleted after 6 months. If you submit a copy of your government-issued ID for account verification purposes, we delete that copy 30 days after submission.³¹⁵

Some social media platforms may share data or information with third parties. These parties may also have different data retention rules in place. The fact that social media users have to agree to the terms and conditions in order to use these services raises questions about accepting third parties' retention policies. Humanitarian Organizations should therefore analyse these policies, assess whether they pose risks to beneficiaries or to the organization itself, and make an informed decision as

³¹³ See [Section 2.7: Data retention](#).

³¹⁴ A. Picchi, "OK, you've deleted Facebook, but is your data still out there?", CBS News, 23 March 2018: <https://www.cbsnews.com/news/ok-youve-deleted-facebook-but-is-your-data-still-out-there/>.

³¹⁵ Facebook data policy.

to whether it is appropriate for the organization to use the platform for its intended objective.

Humanitarian Organizations are also responsible for setting retention periods and/or policies for the data they collect from beneficiaries through social media interactions, groups and pages. They should explain these periods and/or policies to both their staff and beneficiaries.

13.5.4 DATA SECURITY

Humanitarian Organizations should carry out a DPIA (see section 2 above), taking into account the platform's business model, policies, and terms and conditions, the wider ecosystem, and whatever security measures the platform takes to protect the data it processes. While the platform may not share this information openly, analysing previous data breaches, the platform's response and other known vulnerabilities may be a useful starting point. It is also important to understand how the platform processes users' data and what measures it has in place to guarantee that data are kept safe.

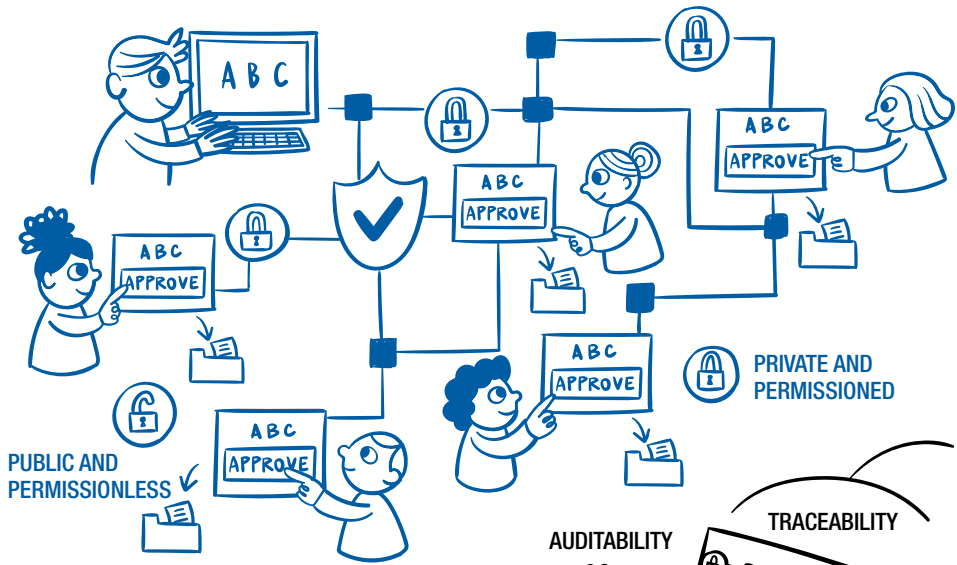
Internally, Humanitarian Organizations are advised to ensure they take appropriate measures to protect the data they collect from beneficiaries, such as protecting data with login and a strong password, granting access on a need-only basis, and training their staff to handle data correctly.

13.6 INTERNATIONAL DATA SHARING

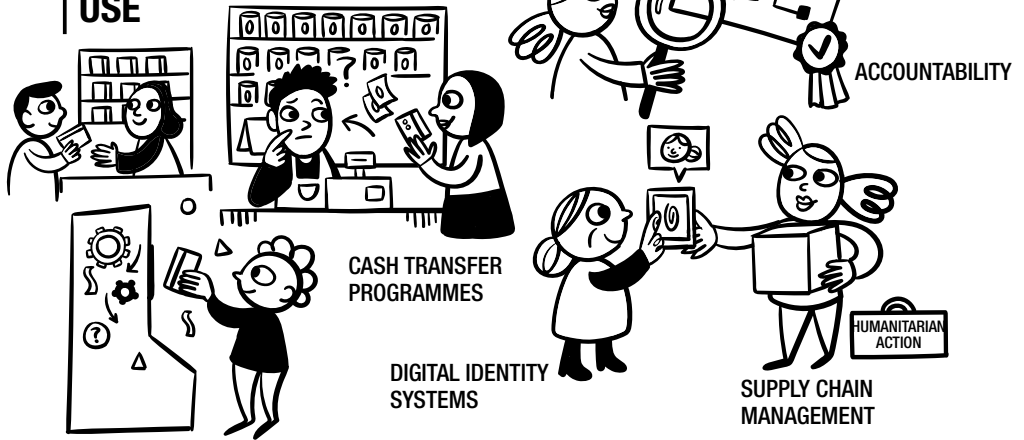
Data processed through social media platforms routinely flows and is accessed across national borders, which raises Personal Data protection concerns. Although recognized contractual mechanisms exist, it can be difficult for Humanitarian Organizations to implement them effectively, especially since social media platforms are often outside their control. That said, organizations must do whatever they can to ensure that the provider has implemented the necessary data transfer arrangements.³¹⁶ Determining applicable law and jurisdiction can also present challenges, since a proper and targeted risk analysis is impossible unless choice of jurisdiction and choice of law are clearly embedded in social media governance.

³¹⁶ See [Chapter 4: International Data Sharing](#).

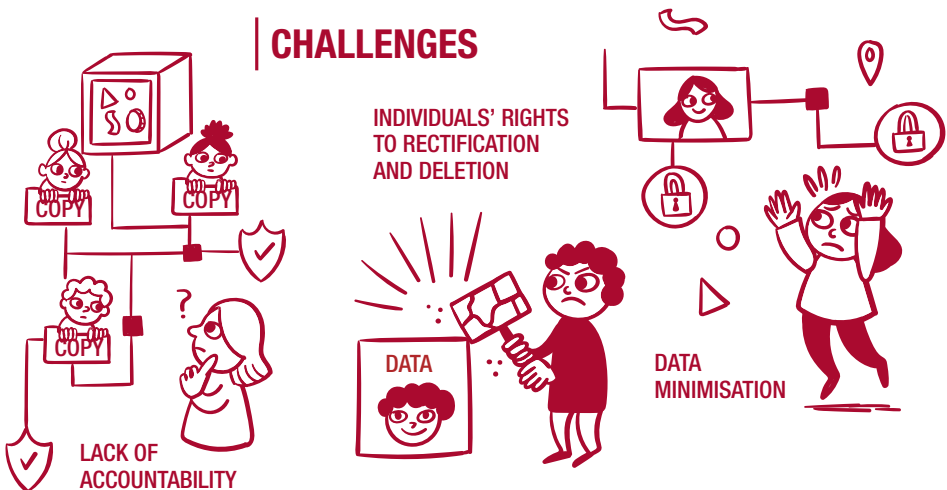
BLOCKCHAIN



POSSIBLE USE



CHALLENGES



CHAPTER 14

BLOCKCHAIN³¹⁷

³¹⁷ The editors would like to thank Robert Riemann (European Data Protection Supervisor), Giulio Coppi (Norwegian Refugee Council) and Bryan Ford (Swiss Federal Institute of Technology in Lausanne) for their contributions to this chapter.

14.1 INTRODUCTION

In recent years, “Blockchain” has become a buzzword and various organizations, including in the humanitarian sector, are trying to find a use for this technology. It has been argued that Blockchain could improve efficiency in humanitarian programmes involving, for example, financial transactions and supply tracing.³¹⁸ It has also been suggested that Blockchain could enhance transparency and trust in information integrity.³¹⁹ However, achieving such improvements could be offset by a number of practical and data protection challenges. These are discussed below, along with any anticipated benefits and risks.

This chapter presents a simplified and easy-to-understand explanation of Blockchain technology, the main parties involved, and its various architectures (sections 1.1 to 1.3). Since Blockchain is a complex technology, this discussion is by no means exhaustive. It merely supports data protection analysis that follows in sections 2 to 7.³²⁰

14.1.1 WHAT IS BLOCKCHAIN?

A Blockchain is “in essence an append-only decentralized database that is maintained by a consensus algorithm and stored on multiple nodes (computers)”.³²¹ This definition includes a number of complex technical elements that are addressed in more detail below. Essentially, Blockchain technology is a special way to store data in a database. As such, any type of data can be stored in a Blockchain, including Personal Data. In a Blockchain, each piece of data is stored one after the other in a chain (which is why it is called “append-only”).³²² This is done by grouping data in blocks and by adding, to each new block, a cryptographic pointer (a reference or link) to the previous block.

The design of Blockchains is guided by a desire to increase security (in the broad sense of the term). In particular, and as mentioned above, Blockchain technology

318 V. Ko and A. Verity, *Blockchain for the Humanitarian Sector: Future Opportunities*, UN-OCHA, 2016, pp. 12–14: <https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf>.

319 Ko and Verity, 2016, p. 8.

320 For more detailed definitions and explanations of Blockchain technology, please refer to: J. Bacon *et al.*, “Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers”, 25 *Rich. J.L. & Tech.*, No. 1, 2018: <https://jolt.richmond.edu/Blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers/>.

321 M. Finck, “Blockchains and Data Protection in the European Union”, *European Data Protection Law Review*, Vol. 4, Issue 1, 2018, p. 17: <https://doi.org/10.21552/edpl/2018/1/6>.

322 Note that this property is the reason why they are also called ledgers: a ledger is a book that stores (traditionally monetary) transactions in append-only mode.

aims to enhance transparency and trust in the integrity of the database. Blockchains are “distributed” and often “decentralized”. While these are two different concepts, they bear a common feature – namely, they indicate that the data being processed is not managed and stored centrally. Here, “distributed” means that there are multiple copies of the database stored on different computers, while “decentralized” means that the power and authority to decide what data are added to the ledger is not held by single entity or individual, but is instead shared between many entities or individuals that have to work together. In this chapter, these entities or individuals are referred to as “validators” (since they, together, validate the data to be stored in the Blockchain). Usually, the higher the number of validators, the more complex the rules they have to follow to reach an agreement. These rules are reflected in a “consensus protocol” (see section 1.2 below for further details).

The computers that hold a copy of the Blockchain are called “nodes” (since they represent nodes in a vast network). Nodes can be passive (only storing an up-to-date copy of the Blockchain) or active. Active nodes are also validators, and are said to be “mining” the data (i.e. participating in the consensus protocol to validate new insertions). Sometimes validators are called “miners” by analogy.

“Users” are the parties who wish to add information to the Blockchain (hence creating data that needs to be validated and recorded on the Blockchain).

A piece of information will only be inserted into the Blockchain once it has been validated. This makes it extremely difficult for a malicious party to add data to the Blockchain, since any addition has to be accepted by the validators first.

Moreover, the blocks of information in a Blockchain are time-stamped and, as mentioned above, contain a cryptographic link (pointer or reference) to the previous block. This means that, even if a malicious party succeeds in changing data contained in a particular block, it also has to modify the following block (as the cryptographic pointer it contains will have changed), as well as all subsequent blocks through to the end of the chain. These changes would unlikely go unnoticed because of a Blockchain’s decentralized design, which means that every validator would have to agree to them. Since it is practically very difficult (but not totally impossible) to change information in Blockchains, they are often referred to as immutable ledgers.³²³

Information added to a Blockchain is digitally signed by a user’s public key (a pseudonymous digital signature of the data source, like a username).³²⁴ Even though public keys by themselves cannot reveal the identity of the person they relate to, they are still considered to be pseudonymized Personal Data as they are linked to one specified individual (the user who added the information). They could be traced

³²³ Finck, 2018, p. 19.

³²⁴ Finck, 2018, p. 19.

back to the individual's IP address, for instance, which could lead to identification.³²⁵ As Blockchains are near-immutable, public keys could potentially remain in the Blockchain for as long as the ledger exists.

Some of the above characteristics of Blockchain technology can be advantageous for Humanitarian Organizations. For example, the decentralized architecture can potentially increase security, since there is no single point of failure or compromise in such systems. This means that potential attackers need to compromise several links in order to compromise the Blockchain as a whole. This set-up increases system integrity because it is claimed to almost always guarantee data immutability.

In light of the fact that information is time-stamped and close to immutable, and the fact that responsibility is shared, it has been argued³²⁶ that Blockchains can be most valuable when:

- they are used to track ownership of complex things over time
- there are multiple groups or parties involved
- there is no well-established or effective central authority (also known as a trusted third party) in place
- groups or parties involved need to work collaboratively
- a record or proof of transactions is required.

These examples show that the one of the main benefits of Blockchain technology is its resistance to a single point of failure or compromise. This is due to the ledger's distributed design, which ensures that multiple nodes have to work together to add new data to the Blockchain. Moreover, because the whole ledger is copied to multiple nodes, it becomes difficult to change information on the ledger and data remains available even if one node is compromised, thereby increasing its integrity.

It is important to note that Blockchain technology will most likely not be needed when there is no issue with the level of integrity (i.e. there is enough trust between the parties involved in a specific programme and there are sufficient levels of auditability), or simply if other current technology offers a sufficient degree of integrity and availability. In such cases, a more traditional solution with a central database, for instance, may prove more efficient, faster and cheaper to implement, and, overall more proportionate from a data protection perspective.

14.1.2 TYPES OF BLOCKCHAIN

Blockchains can be built in different ways, according to system design choices. One key decision, for instance, is whether or not the Blockchain will be public. Although there is no universally agreed definition of each type of Blockchain, the following definitions are more commonly used:

³²⁵ Finck, 2018, pp. 24–25.

³²⁶ Ko and Verity, 2016, p. 9.

Blockchain	Permissionless: Anyone can become a validator (node or miner)	Permissioned: Validators (nodes or miners) are pre-defined and authorized by a governing body
Public: Everyone can access (“see” or “read”) the data stored on the Blockchain and add transactions.	Everyone can read the transactions on the Blockchain (which are public) and participate in the consensus protocol as a validator for new transactions. It is worth noting, however, that data added to the ledger may be encrypted and, therefore, those without the decryption key will not be able to decipher and read its contents. The public keys and time-stamps, however, remain visible to all. This type of Blockchain (public permissionless) is used by Bitcoin.	Everyone can read the transactions on the Blockchain (which are public) but only pre-defined parties can become validators and participate in the consensus protocol to validate new insertions. Such Blockchains could, for instance, help to improve supply-chain transparency, since only those parties involved in the handling of goods would be authorized to alter the ledger (as validators), whereas any member of the public could check the transactions.
Private: Only authorized users can access the data on the Blockchain.	In theory, this type of Blockchain allows only pre-defined parties to access the data stored on the Blockchain, but anyone to participate in the validation of new insertions. In practice, however, this would be hard to implement because validators are able to store a full copy of the ledger. Consequently, it would be difficult to conceive a platform in which validators are not allowed to access the information on the ledger.	Only pre-defined users can access (“read”) the data stored on the Blockchain and only pre-defined validators (not necessarily the same users) can participate in the validation of new insertions.

Besides choosing who can “read” or “write” in the Blockchain, system designers must also decide how validation will take place. Blockchain validation processes are regulated by consensus mechanisms (or consensus protocols), which consist of a set of pre-defined rules that divides trust among the parties. These rules allow them to store data immutably without a central authority (or trusted third party), thereby preserving the integrity of the ledger.³²⁷ In other words, consensus mechanisms define how new information is validated by the parties in the Blockchain and, if deemed valid, added to the ledger.

There are different types of consensus protocol. For example, in Blockchains that use proof-of-work protocols, validators need to earn the right to validate a transaction by solving complex mathematical problems using brute computational

³²⁷ W. Al-Saqaf and N. Seidler, “Blockchain technology for social impact: opportunities and challenges ahead”, *Journal of Cyber Policy*, Vol. 2, Issue 3, 2017, p. 2: <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1400084>.

force, which requires considerable processing power and electricity.³²⁸ In proof-of-stake protocols, meanwhile, the parties have simple voting rights and the weight of their vote may vary according to their stake in the Blockchain.

To illustrate some of the different choices that have to be made when developing a Blockchain, it is useful to think of the system like a corporation. Corporations typically hold board meetings. There need to be rules governing how board members are chosen and who has the right to vote and make decisions. One option is to have a closed group decide who joins and leaves the board (akin to a permissioned Blockchain). Another possibility is to allow anyone to sit on the board as long as they buy enough “stock” in the company to give them voting shares (a proof-of-stake Blockchain). A third option is to decide that anyone can sit on the board as long as they can prove they devoted enough energy to a task in the past ten minutes – an artificial barrier to entry (a proof-of-work Blockchain).

14.1.3 BLOCKCHAIN IN PRACTICE

Scholars and practitioners propose the following advantages and challenges of using Blockchain technology.³²⁹

Advantages:

- There is no need for a trusted third party (a central authority) to maintain the integrity of a shared record: transactions inserted in a Blockchain are verified by participants through a consensus mechanism. The breadth of this benefit, however, varies depending to how the Blockchain is used.
- Eliminating a trusted third party reduces costs. For instance, Blockchain could support cross-border cash transfers directly between the parties to a transaction, removing the need for a bank or another financial institution, which often charges fees.
- A Blockchain acts as an audit trail, since the way data is stored and connected can make it easier to track the origin and movement of physical assets tied to a digital token.³³⁰
- Transparency is increased, especially in public Blockchains, because more parties can access the ledger. In private Blockchains, however, this benefit may be reduced or in some cases non-existent.
- Blockchains improve integrity and availability, since they provide operational resilience and entail no single point of failure or compromise.³³¹

³²⁸ M. Pisa and M. Juden, *Blockchain and Economic Development: Hype vs. Reality*, Center for Global Development, Washington, D.C., 2017, p. 8: https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

³²⁹ For more details, see: Finck, 2018, and Bacon *et al.*, 2017.

³³⁰ Pisa and Juden, 2017, p. 9.

³³¹ Other characteristics of the technology, however, may make it more vulnerable to attacks (see challenges below, as well as section 5.4 on data security).

Challenges:

- An appropriate governance structure needs to be determined for each Blockchain solution.
- Although Blockchains are considered “trustless”, there are parties involved in the system who nevertheless have to be trusted. These include the developers behind the code, as well as designers who create applications that interact with the Blockchain or Cloud Services where data may be stored.
- Blockchain increases the number of access points for possible attacks by malicious parties, thereby posing security risks. Moreover, some consensus mechanisms – albeit not frequently used – accept a transaction as valid when 51% of the validators approve it. So if a consortium of validators gains control of 51% of the nodes, they could jointly take control over the ledger.
- The technology is dependent on internet connectivity.
- Some Blockchains, such as those that use proof-of-work protocols, consume much more electricity than alternative technologies.³³²
- Individuals must be informed, through information notices, about the Processing of Personal Data, and must be able to exercise their rights (such as erasure, rectification and withdrawal of Consent) in respect of their Personal Data.
- Private permissioned Blockchains may be more appropriate for certain types of humanitarian programme (such as cash transfer programming), since these architectures involve a limited number of participants. In some cases, however, this may lead to the reintroduction of trusted parties and to a decrease in transparency.
- Compatibility with data protection requirements in different jurisdictions is a concern (see below).
- While Blockchain technology can help improve transparency in many situations, it does not solve the underlying problems that create so-called “bad data”. In other words, if someone stores unreliable records on a Blockchain, they will remain unreliable and the system will not achieve its potential benefits.³³³

These advantages and challenges of Blockchain have had a significant influence on their use. Blockchains are frequently used to manage transaction histories recording the ownership or custody of, or responsibility for, assets such as cryptocurrencies. They are also used to notarize or assign time-stamps to supply-chain, digital-credential and other documents, as well as to enforce the terms of a contract (through the use of smart contracts).³³⁴

³³² Bacon *et al.*, 2018, p. 15.

³³³ Pisa and Juden, 2017, p. 49.

³³⁴ Smart contracts are a feature of Blockchain that will not be addressed in this chapter. For information on smart contracts see: M. Finck, “Smart Contracts as a Form of Solely Automated Processing Under the GDPR”, *Max Planck Institute for Innovation & Competition Research Paper No. 19-01*, 2019: <https://ssrn.com/abstract=3311370> or <http://dx.doi.org/10.2139/ssrn.3311370>.

14.1.4 HUMANITARIAN USE CASES

Humanitarian Organizations have begun exploring possible applications of Blockchain and have launched pilot projects using the technology.³³⁵ While there is little information available about the benefits and risks that Blockchain technologies bring in such cases, some of the following uses among Humanitarian Organizations have been proposed:³³⁶

- **Cash transfer programming (CTP):**³³⁷ Blockchain could improve the efficiency of CTP through a secure and well-structured transaction record-keeping system, which in turn increase transparency and provide added assurance that data stored in the system have not been tampered with. The application of Blockchain technology to CTP could allow Humanitarian Organizations to make digital cash payments cheaper, more efficient and traceable, as well as interoperable across multiple organizations. In addition, because Blockchain technology is said to provide operational resilience and to entail no single point of failure or compromise, it could make transactions more secure (see section 5.4 below for more information on Blockchain and security).
- **Optimizing and tracking logistics:** Humanitarian supply chains are extremely complex and dynamic, which makes it difficult to monitor them properly. Blockchain technology may offer a way to introduce transparency into these operations. In the case of provision of medical supplies, for instance, a Blockchain may contain a near-immutable, time-stamped record of when the supplies left the warehouse, when they were transported out of the country of origin, when they arrived at the country of destination, when they were received by the local branch of the Humanitarian Organization, and when they reached the destination hospital. Because a public Blockchain provides a publicly visible ledger, it can serve as a transparent data platform that traces the origins, use and destination of humanitarian supplies.
- **Tracking donor financing:** Peer-to-peer tracking and monitoring of donations may make it possible to scale up finance models that cut out the traditional “middleman”³³⁸ (or trusted third party).³³⁹ Such models could reduce transaction costs associated with international humanitarian financing and improve the tracking of donations, including from the general public. However, Blockchain technology could be used to make anonymous donations. This could

³³⁵ For more information on the use of Blockchain in the humanitarian sector, see: G. Coppi and L. Fast, *Blockchain and distributed ledger technologies in the humanitarian sector*, HPG Commissioned Report, 2019: <https://www.odi.org/sites/odi.org.uk/files/resource-documents/12605.pdf>.

³³⁶ Examples taken from Ko and Verity, 2016.

³³⁷ See, for example: International Federation of Red Cross and Red Crescent Societies (IFRC), *Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*, IFRC, 2018: <https://www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-project>.

³³⁸ Ko and Verity, 2016, p. 13.

³³⁹ Finck, 2018, p. 18.

pose a challenge for Humanitarian Organizations with stricter funding policies that require the donating party to be identified.

- **Enhancing shared situational awareness in conflicts:** The Whiteflag Protocol³⁴⁰ (in which the ICRC is collaborating) aims to provide a neutral means of communication for all parties involved in a conflict. Whiteflag is designed to deliver a messaging system in which real-time information on emergencies, local dangers, landmines, population displacement and other issues can be shared in the knowledge that it has not been altered by a malicious party. In this arrangement, none of the participants need to trust one other. Although having this information publicly available could help to locate civilians and assess distinction and proportionality in attacks, it could also be used to target identified groups.

EXAMPLE:

In the Blockchain Open Loop Cash Transfer Pilot Project,³⁴¹ the IFRC and the Kenya Red Cross Society used Blockchain to record cash-based transfers made to beneficiaries from households affected by drought. The idea behind the pilot was to explore the use and added value of Blockchain in CTP. The transfers themselves were made independently from the Blockchain, through a conventional partnership with a local mobile provider and an information management company. Using a private permissioned Blockchain, however, allowed transactions to be recorded almost immutably and in a distributed manner, thereby increasing transparency between the parties (the only ones allowed to access the Blockchain), creating an audit trail (as records were tamper-proof) and increasing record security (as there was no single point of failure or compromise).

Two notable challenges arose during the project. First, it proved difficult to change records when, for example, a disbursement was requested by mistake and a transaction needed to be reversed. Second, because beneficiaries could not receive assistance without Consent, it was questionable whether such Consent was freely given and informed.³⁴²

³⁴⁰ Project website: <https://www.whiteflagprotocol.net>.

³⁴¹ International Federation of Red Cross and Red Crescent Societies (IFRC), *Learning Review: Blockchain Open Loop Cash Transfer Pilot Project*, IFRC, 2018: <https://www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-project>.

³⁴² See [Section 3.2: Consent](#).

14.2 DATA PROTECTION IMPACT ASSESSMENTS

The use of Blockchain in humanitarian programmes may pose many data protection challenges that do not always occur in other contexts. This is one of the main reasons why it is important to carry out a Data Protection Impact Assessment (DPIA) before deciding to implement Blockchain systems. A DPIA can help identify whether it is necessary and proportionate to deploy such a system. If the organization does decide to proceed, the DPIA can also help to identify, address and mitigate the risks and challenges associated with the use of Blockchain. There are many templates and materials for conducting a DPIA,³⁴³ but none of them have thus far been designed specifically for Blockchain in humanitarian contexts. Organizations therefore need to adapt existing DPIA models, or design Blockchain-specific ones.³⁴⁴

A DPIA is a systematic and adaptive process that covers that both general questions relating to the Processing of Personal Data, and questions about to the use of a specific type of technology (in this case, Blockchain). As discussed elsewhere in this chapter, Blockchain presents both advantages and challenges for Humanitarian Organizations. Despite the purported benefits, in most cases no effective improvements have been recorded. During the DPIA process, Humanitarian Organizations should therefore clearly identify the benefits, challenges and risks associated with using Blockchain, comparing them against other technologies. This approach is not new, but it is especially important for an emerging technology like Blockchain.

Since Blockchains can take many different forms, the DPIA must also cover the governance and design of each individual application. Because of the diversity of likely applications and the technical complexity of Blockchain, Humanitarian Organizations may also develop a decision-making framework to help them determine whether to implement Blockchain technologies, and if so, what protections they should implement. Some authors have suggested general decision-making frameworks for implementing Blockchain.³⁴⁵ Yet these generic templates do not take into account the particular data protection concerns raised by Blockchain in the humanitarian sector. For this reason, an alternative, Blockchain-specific decision-making framework is given in the annex to this chapter.

343 See, for example: French Data Protection Authority (CNIL), “Guidelines on DPIA”, 18 October 2017: <https://www.cnil.fr/en/guidelines-dpia>; Information Commissioner’s Office (ICO), *Sample DPIA template*, 2018: https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx?mc_phishing_protection_id=28047-britehqdu81ea0ar3q10.

344 More information about DPIA models and their design can be found in Chapter 5.

345 K. Wüst and A. Gervais, *Do you need a Blockchain?*, paper presented at the Crypto Valley Conference on Blockchain Technology (CVCBT), 2018: <https://eprint.iacr.org/2017/375.pdf>.

Conducting a DPIA can also be vital to identifying an appropriate legal basis for the use of Blockchain. The DPIA process should take into account the impact that a specific type of Blockchain (i.e. the one envisaged in a given situation) may have on Data Subjects' rights and the application of data protection principles. Based on this assessment, Humanitarian Organizations can choose the best solution to minimize potential risks.

The DPIA should give Humanitarian Organizations a clear picture of the impact Blockchain would have in terms of the proportionality of data Processing. Based on this assessment, an organization will be in a position to judge whether there are less intrusive means, such as traditional databases, that could fulfil its needs with less risk to beneficiaries.

As well as assessing the technical design of the system, the DPIA process should also consider the issues and principles detailed in sections 3 to 7 below.

14.3 DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default involves designing a Processing operation, programme or solution in a way that implements key data protection principles from the outset, and that provides the Data Subject with the greatest possible data protections. The key data protection principles in this sense are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation (limited retention)
- integrity and confidentiality (security)
- accountability
- support for Data Subjects' rights by design.

Refer to Chapter 2 for a general description of these principles, some of which are contextualized in the sections below.

At this stage, it is important to take into account the different types of Blockchain, as all options must be considered when designing a model that is compliant with data protection principles.

Private permissioned Blockchains (see Section 1.2 for definitions) are the most restrictive, since one or more parties define(s) who has the right to validate information in the Blockchain and who can access data on the ledger. It may therefore be easier to design private permissioned Blockchains in a way that is compatible

with data protection principles.³⁴⁶ Yet restricting the rights of participants might, in some cases, defeat the very purpose of Blockchain technology by reintroducing a trusted party and, potentially, a single point of failure or compromise.

Public Blockchains, in turn, should always be designed in ways that do not store Personal Data (this is always a preferred option, even for private ledgers). Personal Data could instead be stored “off-chain” (i.e. outside the ledger). Here, the public ledger merely contains a cryptographic pointer confirming that a specific document or piece of information has been stored in a different location (such as on a Humanitarian Organization’s server).³⁴⁷ The data itself is not kept on the Blockchain. Yet even with this design, it is important to remember that public keys belonging to individuals included in the Blockchain will remain Personal Data. Whether or not cryptographic pointers also qualify as Personal Data is a matter of debate.³⁴⁸

14.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

Blockchains, as distributed ledgers, can involve a wide range of bodies and entities. Consequently, it can be difficult to ascertain which parties should be treated as Data Controllers and Data Processors. For clarification, the respective roles of each are detailed below:

- **Data Controllers** determine the means and purposes of Processing. They are accountable for the Processing of Personal Data and are responsible for implementing Data Subjects’ rights. They must compliance with data protection principles and respond to individuals’ requests to exercise their rights to access, rectification and erasure. If there are multiple Data Controllers in the Blockchain, or if new users considered Data Controllers join the Blockchain, their respective responsibilities for the Processing should be set out in a written agreement.

³⁴⁶ M. Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, STUDY: Panel for the Future of Science and Technology, European Parliamentary Research Service (EPRS), 2019, p. 1: [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

³⁴⁷ A cryptographic pointer (also known as a hash pointer) is the one-way mathematical transformation of any given input (a message or a document) into a fixed-length combination of letters and numbers (output). Every time a specific input is hashed, the output is the same, but any slight change to the input (e.g. adding or removing a comma) will produce a completely different hash (Pisa and Juden, 2017). Adding a hash pointer to the Blockchain, therefore, allows a person to verify that a document has been stored, since hashing that document again would produce the same pointer as the one contained in the ledger.

³⁴⁸ Finck, 2019, p. 30.

- **Data Processors** follow the instructions of Data Controllers and are responsible for ensuring data security. They should also inform Data Controllers about which means are being used to process data, and about any problems or complaints that may arise with regard to data integrity, confidentiality and availability.

Each Blockchain architecture (as presented in section 1.2) may have different implications when determining the roles played by different parties operating on the ledger. Importantly, when identifying the Data Controller, determining the purposes of the Processing is a more important factor than choosing the means. With this in mind, and looking at the key parties in Blockchains, one could consider the following arrangements:

- In a permissioned Blockchain, it may be possible to identify a central party (or intermediary) that qualifies as the Data Controller (e.g. system operator that grants “writing” rights), and nodes would qualify as Data Processors.
- In a permissionless Blockchain, there will be no central intermediary, as the network is operated by all nodes in a decentralized manner. Here, every node could potentially qualify as a Data Controller, since they autonomously decide whether to join the chain and pursue their objectives.³⁴⁹ However, there is no unanimity about this conclusion.
- Some argue that nodes are Data Controllers because the fact that they join a Blockchain network can be considered tantamount to determining the purposes of the Processing.³⁵⁰ Others argue that nodes are not Data Controllers.³⁵¹ It is also worth noting that nodes sometimes only see the encrypted version of the data and run software program that does not allow them to alter the ledger. Consequently, they will be unable to “see” what data, including Personal Data, are being processed or make changes to the data and, therefore, cannot comply with data protection obligations of Data Controllers.
- Users (organizations or private individuals deciding to use the Blockchain), in turn, can in some situations qualify as Data Controllers, since they clearly determine the purposes of the Processing, (i.e. recording a specific piece of information onto the Blockchain).³⁵² Furthermore, users choose the means of Processing when selecting a specific version of Blockchain. This interpretation, however, will not apply to every type of Blockchain. This could be the case in a public permissionless Blockchain, but private permissioned Blockchains are more likely to be set up by a consortium of organizations, in which case the consortium will qualify as joint Data Controllers.

³⁴⁹ Finck, 2018, pp. 26–27.

³⁵⁰ Finck, 2018, p. 26.

³⁵¹ J. Bacon *et al.*, “Blockchain Demystified”, *Queen Mary School of Law Legal Studies Research Paper No. 268/2017*, 2017, pp. 64–65: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218.

³⁵² Bacon *et al.*, 2017, p. 64.

The French Data Protection Authority (CNIL) has sought to provide guidance on this matter. According to the CNIL:³⁵³

- Blockchain participants with “writing” rights will be considered Data Controllers when the data they enter is connected to a professional activity.
- Legal persons who “write” data on a Blockchain are considered Data Controllers.
- Miners (or nodes) who do not add data to the Blockchain, but only verify the authenticity of the data (by participating in the consensus protocol), are not Data Controllers because they do not define the means and purposes of the Processing; instead, they can be considered Data Processors, working under the instructions of the Data Controller.
- Blockchain users, meanwhile, can be divided in two types:
 - users who use Blockchain for commercial or professional purposes will qualify as Data Controllers
 - users who use the ledger for private purposes will not qualify as Data Controllers, since this would be considered a purely personal activity falling outside the scope of most data protection laws.

Considering the various interpretations and guidance on this matter, Humanitarian Organizations intending to use Blockchain technology must ensure that the governance of the chosen solution incorporates the concept of Data Controller and Data Processor. They must also determine, as clearly as possible, the responsibilities of each party within a given Processing activity. If it becomes clear that, in a certain situation, it may be impossible for Data Controllers to fulfil their obligations (especially enabling Data Subjects to exercise their rights), an alternative solution should be sought, since the use of Blockchain will most likely be incompatible with data protection principles.

14.5 BASIC DATA PROTECTION PRINCIPLES

As explained above, reconciling the use of Blockchains with basic data protection principles can be challenging. In practice, compatibility between the two will depend on the architecture and design of each Blockchain solution. While this section provides general guidance, organizations must consider the specific features of each application when assessing its compatibility with data protection principles.

14.5.1 DATA MINIMIZATION

By their very nature, distributed ledgers would appear to run counter to the principle of data minimization, which states that the minimum amount of Personal Data should be processed in order to attain the objective and purposes of the

³⁵³ CNIL, *BLOCKCHAIN: Solutions for a responsible use of the blockchain in the context of personal data*, CNIL, 2018: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

Processing.³⁵⁴ This is mainly because data in Blockchains can potentially be stored perpetually, and because a copy of the full ledger is stored in multiple nodes on numerous devices. There may be workaround solutions, however. Personal Data could be stored off the Blockchain while the ledger only keeps a cryptographic pointer to the data that is stored in a different location. In this case, the data will not be stored perpetually on the ledger or shared with all the nodes. The individual or organization that stores the data will retain full control over them and, therefore, will be able to apply the data minimization principle to the off-chain Processing of data without altering the ledger itself. Whether cryptographic pointers also qualify as Personal Data remains a matter of debate.³⁵⁵

14.5.2 DATA RETENTION

The fact that Blockchains are claimed to be immutable distributed ledgers also poses a challenge for the data retention principle.³⁵⁶ Data stored in a Blockchain will be retained indeterminately on multiple computers. The best solution, therefore, would be not to store Personal Data in Blockchains. Personal Data should not, for instance, be stored in public ledgers, since this type of Blockchain can be accessed (or read) by anyone. In particular, Personal Data that are particularly sensitive – such as ethnicity and health records – should never be stored in Blockchains.

14.5.3 PROPORTIONALITY

Proportionality is a core principle of data protection. It generally requires consideration of whether a particular action or measure related to the Processing of Personal Data is appropriate to its pursued aim. Proportionality involves setting out the options and choosing the one that is the least intrusive with regard to the rights of Data Subjects. The complexity of Blockchains can make it difficult to determine whether a particular implementation is proportionate.

As with the data minimization and data retention principles, one way to address proportionality concerns in a public permissionless Blockchain could be to store Personal Data off-chain. Yet adding an off-chain database can mean reintroducing a trusted third party, such as a Cloud Service provider with whom the data will be stored. This, in turn, may negate the supposed benefits of using Blockchain in the first place. The proportionality requirement could, however, be satisfied if the characteristics of Blockchain are essential to achieve the envisaged objective (such as when there is an important need to improve the integrity, transparency and

³⁵⁴ E.g. according to the General Data Protection Regulation (GDPR), Art. 5(1)(c) and (e), Personal Data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”, and “kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed”.

³⁵⁵ Finck, 2019, p. 30.

³⁵⁶ See [Section 2.7: Data retention](#).

availability of an existing solution), and if that objective could not be achieved with a centralized database model (for instance, because the parties do not trust one another). The risks to Data Subjects, however, cannot be disproportionately high in comparison to the aim pursued.

14.5.4 DATA SECURITY

Data security is a key aspect of an effective data protection system.³⁵⁷ Security is often related to three key principles:

- **confidentiality:** the data must only accessible to authorized parties
- **integrity:** unauthorized parties must not be able to modify the data, and the data must not be lost, destroyed or damaged
- **availability:** the data must be available (to authorized parties) when needed.

Blockchains present both strengths and weaknesses when it comes to security across these three aspects. These are detailed, in turn, below.

On the issue of confidentiality, the distributed nature of Blockchains means that the same data are potentially replicated and distributed widely. This leads to increased access points and vulnerabilities. Moreover, even if a Blockchain system uses complex encryption and hashing techniques, advances in quantum computing mean that information could even be decrypted without the decryption key. If, in the future, encryption no longer guarantees the safety and anonymity of the data, all Personal Data stored on a public Blockchain could be exposed. And because, in most situations, data stored on a Blockchain cannot be deleted, the damage can be irreversible. This is yet another reason why it is not recommended to store Personal Data on the Blockchain itself.

With regard to integrity, the immutable character of Blockchain technology and the use of consensus protocols provide a security benefit over centralized databases, not least because “storing sensitive data on centralized servers creates a ‘honeypot’ for would-be hackers and a single point of failure”.³⁵⁸ In Blockchains, however, there is no single point of failure or compromise and, unless an attacker is able to gain control of enough nodes to control the consensus protocol, the system would most likely not be compromised.

On the question of availability, Blockchain is again beneficial because it consists of a distributed ledger stored simultaneously in multiple computers.

Resistance to a single point of failure or compromise is frequently said to be Blockchain’s main added value in relation to security. If that is not an imperative for the organization, then traditional, non-Blockchain technology may be more

³⁵⁷ See [Section 2.8: Data security and Processing security](#).

³⁵⁸ Pisa and Juden, 2017, p. 6.

efficient, faster and cheaper. Secret sharing techniques that are said to enhance the protection of encrypted data in distributed ledgers, for example, can also be used in traditional databases, i.e. they are not exclusive to Blockchain. The technology adds value when integrity and availability are important and when participants do not trust one another.

14.6 RIGHTS OF DATA SUBJECTS

Data Subjects are entitled to certain rights, which allow them to exercise control over their Personal Data. As explained below, however, it can be technically very difficult or impossible to implement these rights on Blockchains.

14.6.1 RIGHT OF ACCESS

Individuals have a right to know whether their Personal Data are being processed by the Data Controller, and to obtain a copy of the Personal Data in question.³⁵⁹ In the humanitarian sector, therefore, when Personal Data is stored on the Blockchain, Humanitarian Organizations should always participate as nodes that hold a full copy of the ledger. That way, they can ensure that the entire database is available at all times, and can inform beneficiaries which data are stored on the Blockchain.

When Personal Data are stored off-chain, meanwhile, the ledger only contains a pointer to the off-chain data. In such cases, the most likely scenario is that Humanitarian Organizations will store the data themselves and should be able to reply to Data Subjects' requests in line with the legal requirements.

14.6.2 RIGHT TO RECTIFICATION

Data Subjects have a right to have incorrect data about them rectified.³⁶⁰ In a Blockchain, however, this can be problematic as it is technically very difficult, albeit not impossible, to change data once it is added to the ledger³⁶¹ (hence the term “immutable”).

If Personal Data are stored on-chain, one way to uphold this right is to add the new, rectified data to the chain – by way of a supplementary statement – while making the previous data inaccessible (for instance by deleting the decryption key needed to access the incorrect data). However, there is no consensus over this solution

³⁵⁹ See [Section 2.11: Rights of Data Subjects](#).

³⁶⁰ See [Section 2.11: Rights of Data Subjects](#).

³⁶¹ D. Conte de Leon *et al.*, “Blockchain: properties and misconceptions”, *Asia Pacific Journal of Innovation and Entrepreneurship*, Vol. 11, No. 3, 2017: https://www.researchgate.net/publication/321811785_Blockchain_properties_and_misconceptions. And the example of the Ethereum hard fork to correct the DAO hack: <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>.

among practitioners and academics. In some cases, it is also possible to insert a new transaction indicating that the old data need to be corrected. The problem with these options, however, is that instead of correcting the original data, they merely add more data to the chain. It is unclear whether this would be accepted as rectification.

In view of these limitations, the best way to deal with these challenges is to store Personal Data off-chain, where it can be rectified without altering the ledger itself. Note that this option would to a large extent reduce the integrity and availability advantages of the Blockchain described above. In other words, if integrity and availability are also important for Personal Data, then a Blockchain-based solution is not recommended.

14.6.3 RIGHT TO ERASURE

The nearly immutable nature of Blockchain stands conceptually in conflict with the right to erasure.³⁶² Various options have been suggested to address this issue. One option, as mentioned above, is to make the data on the chain inaccessible, albeit still present on the chain. This can be achieved, for example, by deleting the decryption key needed to decipher encrypted data. Yet some scholars and practitioners argue that this approach is unsatisfactory because the Personal Data in question, although encrypted, is not deleted (as the right to erasure implies) but merely made inaccessible. This could prove problematic in light of advances in decryption technology (see the discussion on data security above).

Since Personal Data stored off-chain can be rectified and deleted in line with data protection requirements without altering the distributed ledger itself, this is again the preferred option.

EXAMPLE:

If a Humanitarian Organization uses Blockchain for Cash Transfer Programming (CTP), it is likely to ask beneficiaries to have a “wallet” on the Blockchain. The wallet works in almost the same way as a public key, i.e. it can be compared against a username that does not, by itself, identify the beneficiary. The organization will, however, probably maintain an off-chain database or beneficiary management system that links every wallet to a unique beneficiary.

Every time cash is transferred to a beneficiary, a transaction will be added to the Blockchain specifying how much was sent, to which wallet, and when. Once the transaction is validated by the consensus protocol, it is immutably stored in the Blockchain. If beneficiaries request that their data to be erased, it is technically

³⁶² Finck, 2018, p. 30.

impossible to delete their wallet (which, like a public key, constitutes Personal Data) from the chain. One option in this case would be to remove the person from the off-chain database or management system, since this is the only place where the wallet is associated with an individual. Once the personal profile is removed, immediate re-identification should no longer be possible.

14.6.4 RESTRICTIONS OF DATA SUBJECTS' RIGHTS

The above discussion on access, erasure and rectification shows how difficult it can be to exercise data protection rights when using Blockchain technology. Since public permissionless Blockchains are mostly incompatible with Data Subjects' rights, it would seem that the only solution is to store Personal Data off-chain. Yet these rights are not absolute and can, therefore, be restricted. The Data Controller is allowed to take into account available technology and the cost of implementation when Data Subjects requests to exercise their rights. Importantly, however, these restrictions may be acceptable only in exceptional cases.³⁶³ Chapter 2 of this Handbook explains and exemplifies the situations in which Data Subjects' rights can be restricted. Questions remain as to whether it is possible to have a "data-protection-compliant" Blockchain in specific use cases where the Processing legitimately involves derogation from Data Subjects' rights. Even if it is judged legitimate to restrict certain rights, all other data protection principles (data minimization, necessity, proportionality, security, etc.) still apply.

14.7 INTERNATIONAL DATA SHARING

Data processed in Blockchain applications will routinely flow across national borders – especially in public permissionless architectures, which anyone anywhere could potentially join. This raises questions about data protection in Blockchain applications when data are shared internationally.³⁶⁴ Although contractual clauses and other recognized mechanisms exist, such measures may be all-but impracticable in a Blockchain.

Determining applicable law and jurisdiction can also present challenges. The proper and targeted risk analysis as foreseen in Chapter 4 of this Handbook is impossible unless choice of jurisdiction and choice of law are clearly embedded in Blockchain governance (e.g. in private permissioned Blockchains that limit the geographical location of those who can join the chain).

³⁶³ See [Section 2.11: Rights of Data Subjects](#).

³⁶⁴ See [Chapter 4: International Data Sharing](#).

International transfers can be problematic in certain types of Blockchain, such as unlimited public permissionless Blockchains like the one used by the cryptocurrency Bitcoin. Here, there is no central party with control over who joins the system and stores a copy of the ledger. Private permissioned and other architectures can, however, provide more control and therefore help to mitigate such risks. It is therefore possible to attempt to address the transfers issue through Blockchain governance, for instance by embedding data protection guarantees (including by hard-coding them in the Blockchain architecture).

Data Controllers also need to inform Data Subjects if their data have been shared with other parties or transferred to a third country. This is generally not possible – albeit with limited exceptions – in public permissionless Blockchains, since anyone in the world could potentially join the system and store a copy of the ledger. In permissioned Blockchains, however, Data Controllers have more control and should therefore be able to comply with this requirement.

ANNEX: DECISION-MAKING FRAMEWORK FOR BLOCKCHAIN IN HUMANITARIAN ACTION

The following decision-making framework is intended to guide Humanitarian Organizations through the process of implementing Blockchain in humanitarian action:

Step 1:

This step is common to the deployment of any new technology and does not apply exclusively to Blockchain. It consists of an initial information-gathering and scoping exercise that should answer the following questions:

- What problem might a Blockchain solution address?
- To which programme it will apply, and what are the programme's needs?
- Is a Blockchain system the least invasive, most risk-averse and most controllable technology available to address the problem at hand?
- In what context will the Blockchain function?
- Where will it function (in one country or region, worldwide)?
- Who are the stakeholders (beneficiaries, local authorities, financial partners, mobile operators, other Humanitarian Organizations, etc.)?
- What are the objectives of the technology (increase internal efficiency, improve positioning, expand existing programmes, meet donor requirements, manage risks, etc.)?
- What are your existing governance arrangements and IT capacity? Can the technology be implemented, and can the associated risks be managed, under current arrangements and capacity?
- Is it clear how the technology will contribute to the local information ecosystem?

Step 2:

Determine if a Blockchain-based system is necessary to attain the objective(s) of a humanitarian programme or other initiative, taking into consideration the advantages and challenges related to the technology, as identified above, in the particular context in which it will be implemented. Your organization should seek to understand what its needs are, whether or not Blockchain will fulfil those needs, how Data Subjects will experience the system, how their rights will be respected, and whether the same needs could be fulfilled by another system that better protects Data Subjects and their rights. You should ask the following questions:

- Does the order of (trans)actions matter?
- Is there a central authority you can trust?
- Do you need to store data?
- Is there buy-in from your governance/IT support team?
- Do you understand how your system will contribute to the local information ecosystem?

Step 3:

If your organization decides that its objective can only be achieved with a Blockchain solution, you need to determine what type of Blockchain is most appropriate or necessary. Ask the following questions:

- Are there multiple contributors?
- Can you use an “always-online” trusted third party (TTP)?
- Are all contributors known?
- Are all contributors trusted?
- Is public verifiability required?

Step 4:

Consult your DPO, IT support and peers:

- Ask for guidance.
- Make use of the experience of others. For example, consult peers that have developed a similar system or used the off-the-shelf solution you intend to use, and seek advice from Blockchain experts.

Step 5:

Conduct a DPIA to identify and assess Personal Data Processing impacts. A DPIA should include questions such as the following:

- What is the applicable law? Is it applicable to all stakeholders?
- What types of Personal Data are processed? Which of these are necessary for the transaction that will be stored on the Blockchain?
- Is the Processing fair, lawful and transparent?
- What are the alternatives to storing Personal Data on the Blockchain itself? Is off-chain storage possible?

- Are the Data Subjects able to fully exercise their rights? If not, are the restrictions lawful and proportionate?
- Who has the power to determine the governance of the Blockchain?
- How does the platform operate?
- Who can alter the platform and under what circumstances could entries on the ledger be updated?
- What are the risks posed by the chosen technology? How will each risk be treated and mitigated?
- How can individuals exercise their rights?

Step 6:

Implement the principles of data protection by design and by default:

- Both principles require continuous monitoring and revision of technical and organizational measures, taking into account the following: available technology; the cost of implementation; the nature, scope and context of the Processing; the purposes of the Processing; and the risks (of varying likelihood and severity) to the rights and freedoms of natural persons posed by the Processing. A new DPIA should be conducted whenever there is a relevant change in the technology used or the type of data collected.
- Data protection by design involves considering factors such as:
 - compliance with data protection principles (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality)
 - the rights of the Data Subject (e.g. notification, access, erasure, rectification)
 - other data protection obligations (e.g. accountability and security).
- Data protection by default involves considering factors such as:
 - what types and categories of Personal Data are processed
 - the amount of Personal Data processed
 - the purpose for which they are processed
 - the storage period
 - accessibility.

The above framework is summarized in the chart below. If, at the information-gathering stage, your organization concludes that other systems may be more appropriate than Blockchain, then you should not proceed past step 1.

CONNECTIVITY AS AID



POSSIBLE USE

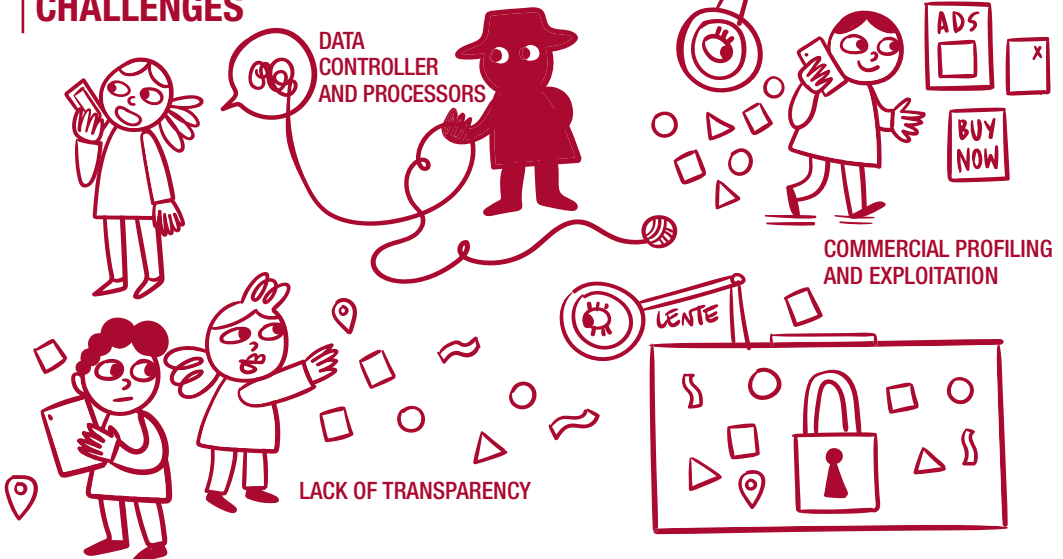


KEEP IN TOUCH
WITH FAMILY MEMBERS



HUMANITARIAN SERVICES

CHALLENGES



CHAPTER 15

CONNECTIVITY AS AID³⁶⁵

365 The editors would like to thank Robert Riemann (European Data Protection Supervisor) and John Warnes (UNHCR), Antonella Napolitano, Ed Geraghty (Privacy International) for their contributions to this chapter.

15.1 INTRODUCTION

In emergencies, staying connected can help beneficiaries get in touch with separated family members, plan safe routes, find shelter, engage with Humanitarian Organizations, and access humanitarian and other services. Yet after disasters, the telecommunications networks on which connectivity³⁶⁶ relies frequently stop working, depriving affected people of the communication channels on which they increasingly rely. Observations have shown that beneficiaries attach considerable importance to connectivity. In 2016, for instance, aid workers assisting migrants in Greece reported that they often asked for internet access before food and water.³⁶⁷ Humanitarian Organizations have recognized the importance of connectivity and developed a range of programmes accordingly.

It is important to differentiate between connectivity *as* aid and connectivity *for* aid. The latter refers to providing connectivity to aid workers so they can carry out their work, while the former relates to providing connectivity to affected people and offering related services as a form of aid in times of emergency or in protracted crises.

This chapter focuses on data protection issues arising from connectivity *as* aid, and at two different levels: community and individual. At the community level, Humanitarian Organizations typically set up hot spots or provide connectivity at community centres. In such cases, organizations usually manage the “pipe” (that is, the physical infrastructure such as cables and fibre bundles needed to provide connectivity), which is shared among users. At the individual level, Humanitarian Organizations may support people in their dealings with connectivity providers, but individuals will have greater responsibility for their own access to connectivity.³⁶⁸ The distinction between these two levels also has implications for the data protection responsibility of Humanitarian Organizations.

15.1.1 OVERVIEW OF CONNECTIVITY AS AID INTERVENTIONS

Various initiatives and organizations are working to provide connectivity in emergencies and address connectivity black spots. Some examples are given below:

- **NetHope**³⁶⁹ provides connectivity solutions in various emergency settings. Working with USAID, the organization brings broadband internet to rural parts of the Middle East, Africa (Botswana, Ghana, Kenya, Liberia, Nigeria and Zambia), Asia (Cambodia and Indonesia) and the Caribbean (Jamaica).

³⁶⁶ For the purposes of this chapter, “connectivity” refers to access to mobile and internet connections.

³⁶⁷ L. Taylor, “Internet Is As Important As Food And Water To Refugees In Greece: Aid Groups”, HuffPost, 22 July 2016: https://www.huffpost.com/entry/internet-is-as-important-as-food-and-water-to-refugees-in-greece_n_57928a22e4b02d5d5ed1ac5b.

³⁶⁸ See for example: UNHCR’s Connectivity for Refugees initiative, Connections, 2019.

³⁶⁹ <https://nethope.org>.

- The **Emergency Telecommunications Cluster (ETC)** is a global network of organizations that work together to provide shared communications services in humanitarian emergencies. The ETC is one of the 11 clusters designated by the Inter-Agency Standing Committee (IASC).³⁷⁰
- UNHCR's **Connectivity for Refugees** initiative helps displaced people and host communities access connectivity, taking a rights-based approach that emphasizes inclusion in national systems.
- Private-sector initiatives:
 - **Loon**³⁷¹ is an initiative initially led by Google to connect people by deploying balloons containing the essential components of cell towers to bring internet access to areas not covered by existing networks. The project aims to expand the reach of 4G wireless broadband (or Long Term Evolution, LTE) by partnering with mobile network operators.
 - **Facebook Connectivity**³⁷² is also involved in a number of initiatives, including Free Basics, which aims to provide free internet access worldwide, and High Altitude Connectivity, which involves advancing the use of high-altitude platform station (HAPS) connectivity systems and satellite technology to bring connectivity to remote areas at lower costs.
 - **CISCO Tactical Operations (TacOp)**³⁷³ deploys a range of technologies and network equipment to provide free communication networks to both Humanitarian Organizations and beneficiaries after disasters. After the 8.1 magnitude earthquake in Nepal in 2015, for instance, Cisco TacOp was on the ground within 72 hours to restore communications.

15.1.2 OPERATIONAL CONTEXT

When starting a connectivity as aid programme, it is important to remember that crises are complex situations, and that the circumstances and people affected will differ from one crisis to the next. Likewise, connectivity programmes will vary according to the context. For some, the emphasis will be on building existing network resilience to future natural disasters or emergencies. For others, the focus will be on establishing connectivity in areas where it has never existed. Although practical arrangements will inevitably differ, organizations will need to consider some common factors no matter what type of programme they are implementing. This first is the regulatory landscape, which will determine what the organization can and cannot do. The second is the commercial and non-commercial organizations currently providing connectivity in the area. Indeed, Humanitarian Organizations often engage with private-sector entities throughout part or all of the connectivity

³⁷⁰ <https://www.etcluster.org>.

³⁷¹ <https://loon.com>.

³⁷² <https://connectivity.fb.com>.

³⁷³ https://www.cisco.com/c/m/en_us/never-better/csr.html.

chain and, as these partnerships have become increasingly common, organizations in both sectors have developed guidelines on how to cooperate with one another.³⁷⁴

When considering partnering with other entities (see section 1.3 below), Humanitarian Organizations are always advised to assess the risks of such partnerships. One way to do so, at least in part, is through a Data Protection Impact Assessment (DPIA) – an exercise that looks beyond data protection issues (see section 2 below) and seeks to ensure that the partnership will cause no harm to affected people.

15.1.3 MULTIPLE STAKEHOLDERS AND PARTNERSHIPS

Humanitarian Organizations may not have the necessary expertise, technology or equipment to implement a connectivity programme alone. This means that they may have to partner with one or more connectivity or technology providers in order to achieve their objectives. These can include non-profit organizations, private enterprises (such as telecommunications providers and technology companies), and NGOs providing connectivity solutions in emergencies.

Aside from considering the other parties involved, it is also important to understand that providing connectivity may be a layered process. As mentioned above, there are two different levels: community and individual. At the individual level, beneficiaries bear a greater responsibility for their own connectivity, since connectivity operators may collect data directly from them.

Once connectivity is established, there are additional (so-called “over-the-top”) services, such as social media services running on top of a phone contract, mobile wallets or mobile money. Some providers of these services may offer their products directly to beneficiaries receiving aid. Here, although the beneficiaries are technically acting as consumers, they are in fact more vulnerable than the average consumer. There are also less visible parties involved in connectivity programmes, such as infrastructure providers and those working on the backhaul to bring connectivity to Humanitarian Organizations or service providers (such as bandwidth providers). Providers can also add deep package inspection (DPI)³⁷⁵ to the network as an added layer of protection. DPI involves filtering unwanted packets (units of data sent from an origin to a destination over the internet) such as viruses or malware. Importantly, however, DPI makes it possible to identify the originator or recipient of content containing specific packets, meaning it can also be used for monitoring and surveillance purposes.

³⁷⁴ See for example: GSM Association (GSMA), “Humanitarian Connectivity Charter”: <https://www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charter>.

³⁷⁵ For more on deep package inspection, see: Tech Target – Search Networking, “deep packet inspection (DPI)”: <https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI>.

All of these organizations and entities operating at different layers of the connectivity programme – backhaul, pipe, over the top and last-mile access – may collect or have access to users' data. This is because additional data and metadata are generated and processed at every layer of connectivity. This Processing by different entities is technically necessary, since sending a message from one location to another usually requires multiple entities knowing its source and destination.³⁷⁶ These metadata (such as connection end points, “likes” and visits) may be accessible to some or all entities in the connectivity chain, which may be able to extract knowledge about humanitarian emergencies and the individuals involved in ways that are difficult for both beneficiaries and Humanitarian Organizations to anticipate.³⁷⁷

Example of connectivity operators collecting data directly from beneficiaries:

A domestic mobile network operator usually has access to the following information for billing purposes: unique identifiers for the SIM card and device (IMSI and IMEI numbers); time and location of transactions, such as calls and messages; and data obtained during SIM card registration.³⁷⁸ The data obtained during SIM card registration may vary considerably from one country to another and according to the type of SIM card purchased (pre-paid or post-paid). Nevertheless, there has been a general tendency towards mandatory registration for all types of card, requiring users to provide Personal Data³⁷⁹ such as a copy of their ID, their national identification number and their date of birth. In some cases, the individual is also cross-checked against a national ID database (India and Pakistan) or has their fingerprints and photograph taken (in Nigeria, for instance).³⁸⁰ Research³⁸¹ has found that, in most cases, refugees and other forcibly displaced people struggle to obtain SIM cards through standard legal channels and resort instead to both formal and informal workarounds that present a number of challenges relating to data flows.

³⁷⁶ International Committee of the Red Cross (ICRC) and Privacy International, *The Humanitarian Metadata Problem: “Doing no Harm” in the Digital Era*, Privacy International and ICRC, 2018, pp. 22–23: <https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf>.

³⁷⁷ ICRC and Privacy International, 2018, p. 23.

³⁷⁸ ICRC and Privacy International, 2018, p. 71.

³⁷⁹ K.P. Donovan and A.K. Martin, “The rise of African SIM Registration: The emerging dynamics of regulatory change”. *First Monday*, Vol. 19, No. 2, 2014: <http://firstmonday.org/ojs/index.php/fm/article/view/4351>; See also the European Court of Human Rights (ECHR) judgment in the case of Breyer v. Germany (application no. 50001/12), 30 January 2020.

³⁸⁰ GSMA. *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*, GSMA Public Policy, 2016: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf.

³⁸¹ UNHCR, “Displaced and Disconnected”, 2019: <https://www.unhcr.org/innovation/displaced-and-disconnected/>.

In this context, Humanitarian Organizations will not have control over the whole connectivity chain and, therefore, cannot guarantee to protect individuals against having their data and metadata misused. The risks that may arise from this lack of control should be evaluated through Data Protection Impact Assessments (see section 2 below) whenever Humanitarian Organizations and their partners play an active role in improving connectivity for affected communities. As a mitigating measure, some Humanitarian Organizations provide affected people with information and guidance on digital security.³⁸² But if the risk proves too great, Humanitarian Organizations may have no choice but to opt not to provide connectivity.

15.2 DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA)³⁸³ is carried out to identify, evaluate and address the risks posed to Data Subjects by the Processing of their Personal Data in connection with a project, policy, programme or other initiative. It should ultimately lead to measures promoting the avoidance, minimization, transfer or sharing of data protection risks. Before launching technology programmes that involve the Processing of Personal Data, Humanitarian Organizations should conduct a DPIA to assess the possible consequences, which could include unlawful use of beneficiaries' data by partners and government interference with the network.

Before entering into a partnership for a connectivity programme, a Humanitarian Organization should assess potential partners and their privacy policies, as well as the legal obligations to which they are subject, in order to fully understand how they process beneficiaries' data. Once the organizations has a clear picture of the connectivity landscape, the parties involved and the services that provide, it may be in a position to draft standard guidelines or requirements explaining the services it needs, including technical specifications and privacy requirements. This could help organizations engage with partners and shorten the time between engagement and agreement in times of emergency.

It is also important to remember that, in the humanitarian sector, beneficiaries are especially vulnerable and the risk of harm is high. For these reasons, the DPIA should give due consideration to Data Subjects' other fundamental rights.³⁸⁴ Since

³⁸² For more on data security, see [Section 2.8: Data security and Processing security](#).

³⁸³ See Chapter 5: Data Protection Impact Assessments (DPIAs).

³⁸⁴ See: EU Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (wp248rev.01)*, 2017: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711; and R. Gellert, “Understanding the notion of risk in the General Data Protection Regulation”, *Computer Law & Security Review*, Vol. 43, Issue 2, 2018: <https://doi.org/10.1016/j.clsr.2017.12.003>.

Humanitarian Organizations operate in accordance with humanitarian principles, it may also be appropriate to consider the rights and freedoms of all members of a given group or community when setting up connectivity programmes, including non-data-related rights. A DPIA could, for instance, examine issues around unequal access to the network³⁸⁵ and the potential exclusion of certain groups that are not digitally literate. It is also important to consider that some of the partners Humanitarian Organizations work with have business models that are based on the monetization of data, which may be incompatible with humanitarian principles. Organizations may also be unwilling to engage with some private-sector partners because of the reputational risk that doing so can carry. If the DPIA indicates that a connectivity programme could create more problems than it solves, it may be appropriate to decide not to engage.

15.3 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

A Data Controller is the person or organization who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. A Data Processor, meanwhile, is the person or organization who processes Personal Data on behalf of the Data Controller. These concepts are defined and discussed at greater length in Chapter 2.

When Humanitarian Organizations set up and operate connectivity programmes, they can act as either Data Controllers or Data Processors, depending on the role that they and other partners play in a given programme. This distinction is important when attributing responsibilities for data Processing.

Since data are collected at different layers of a connectivity programme, it is important to map data flows at each layer, identifying who is collecting them, what the purposes are, how long the data are retained, and with whom they are shared. This mapping exercise will help to identify what role each party, including the Humanitarian Organization, plays in deciding how data are processed – and, therefore, whether each one is acting as a Data Controller or a Data Processor.

385 E.g. young children and elderly people might not be able to benefit from connectivity programmes or access services that require connectivity as they may lack computer literacy. In addition, “[w]omen in low- and middle-income countries are 10% less likely to own a mobile phone, and are considerably less likely than men to use more transformative services. For example, women in low- and middle-income countries are 26% less likely than men to use mobile internet, and 33% less likely to use mobile money.” Source: GSMA, *Connected Women: The Gender Analysis & Identification Toolkit. Estimating subscriber gender using machine learning*, GSMA, 2018, p. 6: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Gender-Analysis-and-Identification-Report-GAIT-August-2018.pdf>.

If a Humanitarian Organization determines the final objective (purpose) of the programme (such as establishing connectivity) and chooses a specific partner to implement it (means), it qualifies as a Data Controller. This means that the organization has a range of obligations, including responding to requests from Data Subjects wishing to exercise their rights.³⁸⁶ In some cases, Humanitarian Organizations and partners from other sectors will determine the purpose and means of the programme together and, therefore, act as joint controllers. In such situations, the joint controllers must set out their respective responsibilities, including the handling of Data Subjects' requests, in a written agreement.

15.4 BASIC DATA PROTECTION PRINCIPLES

15.4.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

When Personal Data are required to access connectivity services, or generated in the process, an appropriate legal basis for the Processing of these data is necessary. Such legal bases are listed in Chapter 3 of this Handbook, which also explains the challenges associated with using Consent as a legal basis in humanitarian settings. Consent in humanitarian contexts may not always be considered freely given, since beneficiaries may feel compelled to consent when that is the only way to receive a specific service (in this case, connectivity). Moreover, the complexity surrounding connectivity as aid might make it difficult to rely on a properly informed Consent, since Data Subjects with lower levels of digital literacy might not be able to understand all aspects of the Processing. Here, Humanitarian Organizations and service providers should seek a different legal basis for data collection and Processing, such as those listed below:

- **Public interest:** This may be an option for an organization that has a specific mandate to establish connectivity.³⁸⁷
- **Legitimate interest of the Humanitarian Organization:** This basis could also be considered where establishing or re-establishing connectivity is in line with the organization's mission, and where doing so could help beneficiaries access other essential services and improve coordination of the humanitarian response. This basis would only apply, however, if the interest(s) pursued by the organization and the anticipated benefits of the Processing are not outweighed by the rights and freedoms of the individuals in question.³⁸⁸
- **Legal obligation:** Some jurisdictions may require connectivity service users to be registered. Here, the legal basis for processing users' data for registration would be compliance with a legal obligation.³⁸⁹

³⁸⁶ See [Section 2.11: Rights of Data Subjects](#).

³⁸⁷ See [Chapter 3: Legal bases for Personal Data Processing](#).

³⁸⁸ See [Section 3.5: Legitimate interest](#).

³⁸⁹ See [Section 3.7: Compliance with a legal obligation](#).

15.4.2 DATA SECURITY

Mobile network operators play an important role as providers of critical connectivity infrastructure. In emergencies, for instance, being able to communicate with ambulances and other health-care providers is vital to effective incident response. These operators are required to implement technical and organizational security measures in order to protect communication networks and keep the data they carry secure. These measures, which will depend on the degree of risk, include encryption and other technical ways of ensuring the confidentiality, integrity and availability of collected data, as well as the overall resilience of processing systems and services.³⁹⁰

Some metadata stored on individual devices, however, may not be encrypted and may require alternative security measures.³⁹¹ Wherever possible, Humanitarian Organizations and individuals should routinely review and update the measures they take, in order to account for the development of new security technologies, and to ensure a level of data protection and security that is appropriate to the degree of risk involved in the Processing of Personal Data. It is important to remain mindful that some entities or organizations may have an interest in accessing the data and metadata generated in connectivity programmes for non-humanitarian purposes, such as commercial targeting and exploitation, or surveillance.

EXAMPLE:

Germany and Denmark have passed laws that allow the authorities to carry out a detailed forensic analysis of asylum seekers' smartphones. The data and metadata extracted from their devices can be used "to verify claims made in their asylum applications or to obtain new information about their identity, their story, the route they took, etc."³⁹² Similar legislation has been passed in Belgium and proposed in Austria.³⁹³ In practice, such laws could mean that data generated through connectivity programmes end up being used for purposes that, even if legitimate, may not be compatible with the principles by which Humanitarian Organizations abide.

Current surveillance methods can be quite sophisticated and obtain substantial amounts of data and metadata about users of a given network.³⁹⁴ This is particularly concerning, since metadata can be used to infer information that an individual has

³⁹⁰ For more on data security, see [Section 2.8: Data security and Processing security](#).

³⁹¹ ICRC and Privacy International, 2018, p. 25.

³⁹² ICRC and Privacy International, 2018, p. 62.

³⁹³ ICRC and Privacy International, 2018, p. 62.

³⁹⁴ See for example: B. Schneier, "China Isn't the Only Problem With 5G", Foreign Policy, 10 January 2020: <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>.

not agreed to share, and make predictions about their behaviour, which would mean that data generated in the process of humanitarian services could end up being used as highly valuable information in conflict.

In some cases, a Humanitarian Organization – depending on its mandate – may need to cooperate with national or foreign government authorities on a given connectivity programme. This type of cooperation can be in the interest of beneficiaries, such as when medical data are shared with health authorities to facilitate the provision of medical aid and public health. Humanitarian Organizations should be transparent with beneficiaries about any such cooperation arrangements, and make clear that their data may be shared with national or foreign authorities.

Humanitarian Organizations should negotiate security measures with their partners to ensure the highest level of security throughout the entire connectivity chain – including those parts of the chain outside the organization's control.

15.4.3 DATA RETENTION

Personal Data must not be kept for longer than is necessary to fulfil the purposes for which they were collected or to comply with applicable legal obligations.³⁹⁵ This means that Personal Data should always be deleted or anonymized as soon as they are no longer needed. In connectivity programmes, however, the various partners may have different roles, policies and needs that could impact how they Process data, including how long they retain them for. Again, it is important at the outset to establish a written agreement setting out each party's responsibilities and data retention policies. This will ensure that Humanitarian Organizations fully understand what data are being held by each partner at a certain point in time, and where they are being stored.

Mobile network operators frequently have to retain data about users for periods specified in national law. Requirements such as these are intended, for instance, to give law enforcement authorities access to data in case a crime is committed. Humanitarian Organizations should therefore analyse which data are actually needed to deploy the programme and, as far as they can, avoid the collection of any unnecessary data. If only a minimum amount of data is collected, then only a minimum amount can be retained.

³⁹⁵ See [Section 2.7: Data retention](#).

15.4.4 INFORMATION

In connectivity programmes, Data Subjects should be informed in clear and plain language about what data relating to them are being collected, for what purpose and through which means. This is especially important in situations where it may not be obvious to Data Subjects that their data are being collected, such as when metadata are generated or when the data collected are inferred data (information that can be deduced from data explicitly given by the Data Subject or from other observations). Individuals should also be told whom they can contact to exercise their rights. This information will enable them to make informed decisions about whether or not to use a specific service, and to understand how to proceed when they wish to exercise their rights.

In the interest of transparency and full disclosure, Humanitarian Organizations are advised to inform Data Subjects about the third parties involved in the programme, which activities they are responsible for, and how to contact them. They should also be informed about the actual and potential negative consequences and risks associated with receiving and using connectivity services, and with connectivity programmes in general. The example set by UNHCR, which informs individuals of the privacy risks associated with the El Jaguar campaign, is a helpful model to follow.³⁹⁶

15.5 INTERNATIONAL DATA SHARING

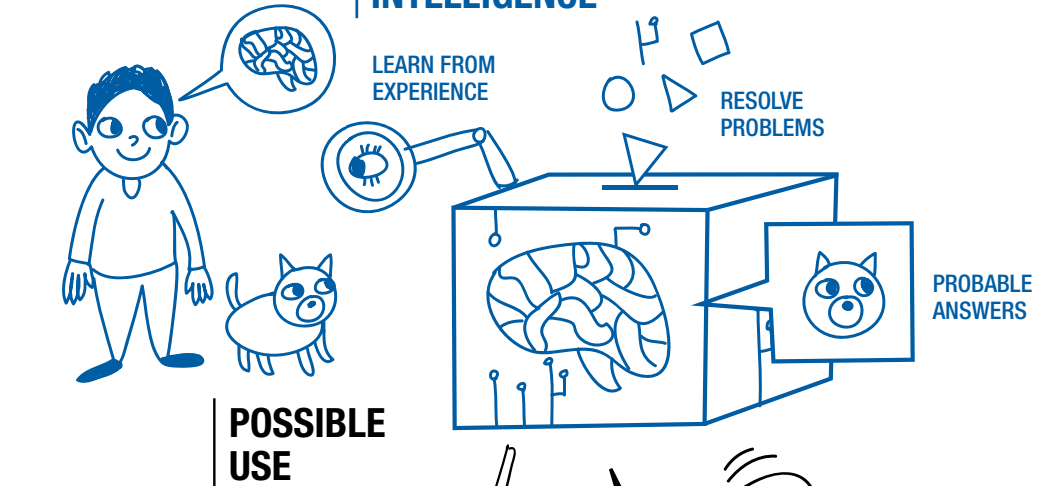
Data processed online routinely flows across national borders. This raises Personal Data protection concerns in relation to connectivity programmes. Although recognized legal mechanisms exist, such the use of contractual clauses, it can be difficult for Humanitarian Organizations to implement them effectively, especially since connectivity solutions are often outside their control. That said, organizations should do whatever they can to ensure that the provider has implemented the necessary data transfer arrangements.³⁹⁷

³⁹⁶ See <https://www.facebook.com/ConfiaEnElJaguar/videos/874221649451680/>.

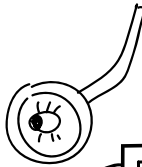
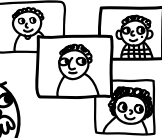
This campaign video provides tips on privacy and profile safety on social media.

³⁹⁷ See [Chapter 4: International Data Sharing](#).

ARTIFICIAL INTELLIGENCE

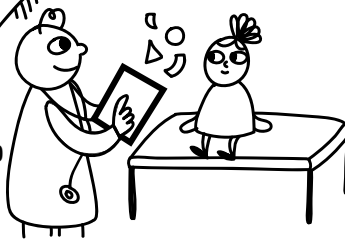


FINDING PERSONS
SEPARATED FROM
THEIR FAMILIES



PROCESS IMAGES
TO ASSESS
DAMAGES

IDENTIFYING
CATEGORIES OF
PEOPLE IN NEED
OF AID

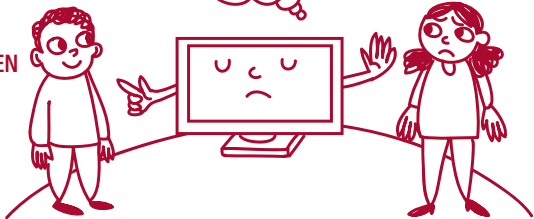


CHALLENGES



DETECTING
BIASES

DECISIONS
BASED ON AI-DRIVEN
ANALYSIS



UNDERSTANDING
THE CONCLUSIONS



ATTACKING
INTEGRITY
OF DATA



CHAPTER 16

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING³⁹⁸

398 The editors would like to thank Alessandro Mantelero (Politecnico di Torino) for his contributions to this chapter.

16.1 INTRODUCTION

This chapter explores the data protection challenges associated with the use of Artificial Intelligence and Machine Learning systems in the humanitarian sector. Some of these challenges relate to the much-debated topic of automated decision-making, while others arise from the fact that such systems frequently rely on the heavy usage of data, sometimes including Personal Data. The sections that follow first give a basic explanation of the technology in question, then identify the related data protection challenges and provide guidance for Humanitarian Organizations on how to address some of these challenges.

16.1.1 WHAT ARE ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING?

While there is no single, universally accepted definition of the term, Artificial Intelligence is generally understood as “[a] set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being”.³⁹⁹ In its current form, it aims to allow technology developers “to entrust a machine with complex tasks previously delegated to a human.”⁴⁰⁰

Machine Learning, in turn, is a specific form of Artificial Intelligence that can be defined as the study of algorithms that get better at completing a certain task over time, with experience in the form of machine-readable data.⁴⁰¹ An algorithm receives more and more data representing the problem it is trying to solve and ‘learns’ from such data. There are, however, other Artificial Intelligence techniques that are less reliant on data because they ‘learn’ in different ways.⁴⁰²

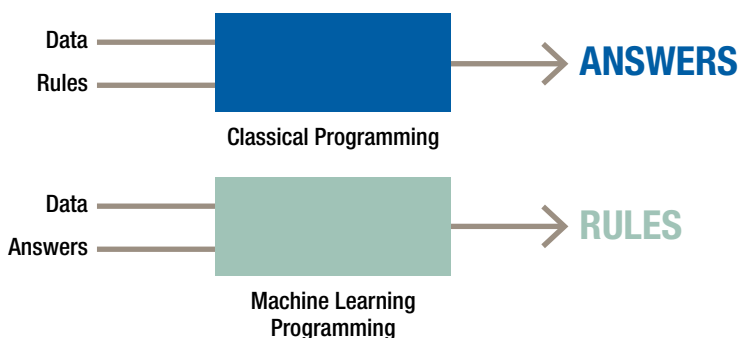
Regardless of their learning method, all forms of Artificial Intelligence share a common feature: they are not a set of instructions for a machine to complete a particular task, but rather a set of instructions for the machine to generate strategies or solutions to complete that task. This is shown in the model opposite:

³⁹⁹ Council of Europe (CoE), Glossary on Artificial Intelligence: https://www.coe.int/en/web/artificial-intelligence/glossary?mc_phishing_protection_id=28047-brbqhtidu81d093fnuog.

⁴⁰⁰ CoE, Glossary on Artificial Intelligence.

⁴⁰¹ T. Mitchell, *Machine Learning*, McGraw-Hill, New York, 1997, p. 2.

⁴⁰² Examples of these methods include Bayesian networks and rule-based engines. These methods, however, are not addressed in this chapter.



Source: F. Chollet, *Deep Learning with Python*, Manning Publications, 2017

Machine Learning is a form of Artificial Intelligence and, in recent years, has attracted the vast majority of Artificial Intelligence investment. For these reasons, the term ‘Artificial Intelligence’ will be used throughout this chapter to include both Artificial Intelligence and Machine Learning solutions. Whenever a point relates to a specific technique, this will be made clear.

16.1.2 HOW DO ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING WORK?

There are many different Artificial Intelligence techniques in existence. Some process Personal Data, while others do not. Yet most solutions, especially those using Machine Learning, function as follows:

1. Selected data expected to contain specific patterns or similarities (training data) are presented to the system.
2. Artificial Intelligence techniques identify the patterns and determine which features are relevant for the classification of these patterns or similarities and for making predictions about new data.
3. “A model is generated that can recognize the patterns that emerge when fresh data is processed by the model” to make predictions or classifications.⁴⁰³

While most types of Artificial Intelligence rely on being fed large amounts of data, some only require limited volumes of data to function. In order to understand the most important data protection implications explained in section 3 of this chapter, it is important to understand the different ways in which Artificial Intelligence solutions ‘learn’:

- **Supervised learning:** under this model, training data is labelled (the analyst assigns a ‘class’ to each piece of sample data). For instance, sample images of animals are tagged with labels such as ‘dog’, ‘cat’ or ‘parrot’ and fed into the

⁴⁰³ The Norwegian Data Protection Authority, *Artificial intelligence and privacy*, 2018, p. 7: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

system. Typically, the ultimate objective will be for the algorithm to be able to classify new (unseen) images into one of the learned classes. This type of learning can also be used, for example, to predict a value based on different parameters (or features), such as valuing a house based on the number of rooms, size and/or year of construction. In both cases, the principle is to determine the best mathematical function that will properly separate the data into its correct classes or evaluate correct values.

- **Unsupervised learning:** in this case, no labels are fed into the system. The idea is for the algorithm to discover similarities or patterns in a dataset and to create the labels (or classes) itself. Different methods are applied to organize the data into 'clusters'. There are no right or wrong answers.
- **Reinforcement learning:** this approach requires little or no training data. Instead, it relies on a method of reward and punishment, whereby "the system is given a 'reward' signal for when it accomplishes what the designer wants, or a step that advances the process toward the outcome the designer described. When the system does something wrong (fails to efficiently advance toward the desired outcome), it is simply not rewarded."⁴⁰⁴

Once a solution is trained by one of the methods mentioned above,⁴⁰⁵ it creates a model that will be used to analyze and/or make predictions about new and unseen data. The models generated by Artificial Intelligence can be static or dynamic. Static models will not change over time and will always apply the model developed with the training data. This allows the developer to maintain full control of the model but stops the solution from refining itself over time. Dynamic models, on the other hand, avail themselves of input data to adjust to changes and refine their outputs.⁴⁰⁶

Since most Artificial Intelligence solutions learn from the data that passes through them (either during training or, in dynamic models, also during deployment), the resulting models will retain part of the data that was used to develop and/or improve them. This means that, in some cases, malicious parties who attack and successfully gain control of the system could access the training data (or the data used during the deployment of the solution in dynamic models). More information on possible attacks on Artificial Intelligence solutions can be found in the discussion on data security below (section 3.5).

⁴⁰⁴ The Norwegian Data Protection Authority, 2018, p. 18.

⁴⁰⁵ This chapter does not address all possible Artificial Intelligence learning methods. For more information on methods not mentioned here (such as neural networks), see for example: L. Hardesty, "Explained: Neural networks", MIT News, 14 April 2017: <http://news.mit.edu/2017/explained-neural-networks-deep-learning-0414>; and Future of Privacy Forum, *The Privacy Expert's Guide to Artificial Intelligence and Machine Learning*, 2018: https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf.

⁴⁰⁶ For more information, see: The Norwegian Data Protection Authority, 2018, p. 10.

16.1.3 ARTIFICIAL INTELLIGENCE IN THE HUMANITARIAN SECTOR

Recent growth in available data and processing power has greatly increased the number of Artificial Intelligence applications in everyday life.⁴⁰⁷ Artificial Intelligence is present, for example, in voice-activated digital assistants, in biometric recognition systems that unlock phones or allow access to buildings, in traffic routing applications, in purchase or viewing recommendations on online platforms, and in many other features of online tools and services and smart devices. The technology can also be applied to a great variety of tasks, including medical diagnosis, image recognition, stock market prediction and gaming.

Artificial Intelligence can also help facilitate humanitarian work, and activities linked to it or with similar features, and make it more effective and efficient. Some existing and potential applications are detailed below:

- **Reading public opinion:** In Uganda, the UN Global Pulse programme piloted “a toolkit that makes public radio broadcasts machine-readable through the use of speech recognition technology and translation tools that transform radio content into text.”⁴⁰⁸ This tool, developed by the Pulse Lab Kampala, aims to identify trends among different population groups, particularly those in rural areas. The rationale behind the initiative is that these trends could then provide government and development partners with a better understanding of public opinion on the country’s development needs, which could then be taken into consideration when implementing development programmes.
- **Identifying and locating missing children:** It has been reported⁴⁰⁹ that India’s National Tracking System for Missing & Vulnerable Children identified nearly 3,000 missing children within four days of launching a trial of a new facial recognition system that matches the faces of missing individuals with photographs of children living in children’s homes and orphanages.
- **Tracking attacks on civilians and human rights violations:** Amnesty International’s Decode the Difference project⁴¹⁰ recruited volunteers to compare

⁴⁰⁷ Centre for Information Policy Leadership, *First Report: Artificial Intelligence and Data Protection in Tension*, 2018, p. 4: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

⁴⁰⁸ UN Global Pulse, “Making Ugandan Community Radio Machine-readable Using Speech Recognition Technology”, 2016: <https://www.unglobalpulse.org/projects/radio-mining-uganda>.

⁴⁰⁹ A. Cuthbertson, “Indian police trace 3,000 missing children in just four days using facial recognition technology”, *The Independent*, 24 April 2018: <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>; see also: *The Times of India*, “Delhi: Facial recognition system helps trace 3,000 missing children in 4 days”, 22 April 2018: http://timesofindia.indiatimes.com/articleshow/63870129.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. For the system’s official website, see: <https://trackthemissingchild.gov.in/trackchild/index.php/index.php>.

⁴¹⁰ Amnesty International, “Amnesty Decoders”: <https://decoders.amnesty.org/>.

images of the same location at different time periods to identify damaged buildings, which could potentially demonstrate systematic attacks against civilians. In the future, the data could be used to train Machine Learning tools to analyse the images, thereby speeding up the process and increasing capacity.

- **Preventing and diagnosing disease:** “Since the 1990s, AI [Artificial Intelligence] has been used to diagnose various types of diseases, such as cancer, multiple sclerosis, pancreatic disease and diabetes.”⁴¹¹ More recently, Microsoft’s Project Premonition was developed to detect pathogens before they cause outbreaks. The project deploys robots that aim to monitor the presence of mosquitoes in an area, make predictions about their distribution, and capture targeted species. Through Machine Learning techniques, the captured mosquitoes are searched for pathogens they may carry from animals they have bitten.⁴¹²

16.1.4 CHALLENGES AND RISKS OF USING ARTIFICIAL INTELLIGENCE

Despite their potential, Artificial Intelligence applications carry challenges and risks. Besides data protection concerns (see section 3 below), all the above-mentioned use cases also present practical implementation challenges. For example, Artificial Intelligence-based image recognition software used to identify missing people may provide too many false positives. These false matches could not only create confusion among case workers, but also potentially give false hope to families. Other systems could be more accurate but potentially miss positive matches (known as false negatives). While false negatives may not be much of an issue in commercial applications, they can have devastating consequences in the humanitarian sector. If an organization misidentifies a child who has lost contact with their parents, this can cause harm to the entire family.

As the above discussion highlights, Artificial Intelligence can pose risks to beneficiaries. For instance, if Artificial Intelligence is used to identify the right target population for a particular humanitarian programme, and the solution does not make a correct identification, people who would otherwise be entitled to participate in the programme could be excluded. This has happened in practice in Sweden, where thousands of unemployed people were wrongly denied benefits by a government system that used Artificial Intelligence.⁴¹³

⁴¹¹ H.M. Roff, “Advancing Human Security through Artificial Intelligence”, Chatham House, 2017, p. 5: <https://www.chathamhouse.org/publication/advancing-human-security-through-artificial-intelligence>.

⁴¹² Microsoft, “Microsoft Premonition”: <https://www.microsoft.com/en-us/research/project/project-premonition/>.

⁴¹³ T. Wills, “Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed”, Algorithm Watch, 25 February 2019: <https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/>.

Since most Humanitarian Organizations will acquire off-the-shelf solutions rather than developing their own models, there is a risk that algorithms could deliver unexpected or unreasonable results. Likewise, vendor lock-in poses a risk because switching solutions may be costly. Organizations could also be targeted by commercial ventures that are primarily interested in gaining access to and exploiting the large datasets they hold, sometimes at great risk to the individuals and communities to whom the data relate.

Bias poses another risk to the effectiveness of Artificial Intelligence, especially in specific humanitarian contexts (see section 3.2.2 below). Since most (but not all) solutions are trained against large amounts of data, it is important to select a dataset that is fit for the intended goal. When the solution is used to identify patterns or make predictions about individuals or specific communities, the training dataset will most likely need to include Personal Data.

As with many other technologies, the concept of ‘garbage in, garbage out’⁴¹⁴ also applies to Artificial Intelligence, and using unfit, inaccurate or irrelevant data may affect the accuracy of the solution. This is particularly challenging for humanitarian organization as off-the-shelf algorithms will extremely rarely be bespoke to their contexts. For instance, if a Humanitarian Organization wants to develop facial recognition software to help find missing people, the training datasets will need to be sufficiently broad to ensure that racial variations in physical features are integrated to maximize the precision of the matching function.

16.2 DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) involves identifying, evaluating and addressing the impacts on Data Subjects and their Personal Data of a project, policy, programme or other initiative that entails the Processing of such data.⁴¹⁵ It should ultimately lead to measures that avoid, minimize, transfer or share risks associated with the Processing activities. A DPIA is a continuous process and should follow a project or initiative that involves the Processing of individuals’ data throughout its lifecycle. Given the limits to transparency in the use of Artificial Intelligence (as explained in more detail below in section 3.2.3), DPIAs can help increase beneficiaries’ acceptance and use of Artificial Intelligence solutions

⁴¹⁴ According to the free online dictionary of computing (<http://foldoc.org>), the concept of garbage in, garbage out relates to the fact that “computers, unlike humans, will unquestioningly process nonsensical input data and produce nonsensical output”. The term is also used to refer to “failures in human decision-making due to faulty, incomplete, or imprecise data”.

⁴¹⁵ See [Chapter 5: Data Protection Impact Assessments \(DPIAs\)](#).

by Humanitarian Organizations. Since the use of Artificial Intelligence can pose substantial data protection risks to individuals, an organization should carry out a DPIA before making a decision to implement such a solution. The ethical implications of Artificial Intelligence, as discussed below in section 8, should also be considered when conducting a DPIA.

16.3 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

As mentioned above, most Artificial Intelligence solutions need to process large amounts of data – both personal and non-personal – in order to function properly. It can be difficult, however, to know when Artificial Intelligence solutions process Personal Data and, consequently, when data protection principles apply. This is because Artificial Intelligence solutions are increasingly capable “of linking data or recognizing patterns of data [that] may render non-personal data identifiable.”⁴¹⁶ This means that, in some cases, Artificial Intelligence solutions can re-identify pseudonymized data, i.e. render data identifiable by broadening “the types of and demand for collected data, for example, from the sensors in cell phones, cars and other devices,” as well as by providing “increasingly advanced computational capabilities to work with collected data,” thus providing opportunities to combine it in a way to reliably identify individuals.⁴¹⁷ As with other systems that process Personal Data, due consideration must be given to the solution’s architecture, and to the context in which it will be used, when determining whether and how data protection principles apply.

16.3.1 PURPOSE LIMITATION AND FURTHER PROCESSING

Applying the purpose limitation principle⁴¹⁸ to Artificial Intelligence and Machine Learning solutions is challenging because these technologies may have the capacity to process data in ways they were not originally planned, and, therefore, achieve a different purpose than the one originally intended. This is mainly due to the very nature of Machine Learning, which is to test and reveal various correlations within an analyzed dataset. As a consequence, these solutions are readily able to infer new things from the data’s features.

⁴¹⁶ Centre for Information Policy Leadership, 2018, p. 11.

⁴¹⁷ Centre for Information Policy Leadership, 2018, p. 11.

⁴¹⁸ See [Section 2.5.2: The purpose limitation principle](#).

EXAMPLE:

In 2012, researchers found that when Artificial Intelligence algorithms analyzed a person's Facebook 'likes', with no further information from that person, the solutions could "automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender."⁴¹⁹ More specifically, the solution correctly discriminated "between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases."⁴²⁰ In this particular case, the solution was being asked to make these correlations. Yet in other situations, Artificial Intelligence solutions may draw such inferences on their own and reveal sensitive information about a person even when that was not the developer's intention.

The purpose limitation principle requires organizations to determine a clearly defined goal for the Processing of Personal Data and to consider the means and information needed to achieve such a goal. Yet with Artificial Intelligence, they must also consider whether the solution might produce an unwanted outcome. If it is foreseen that the solution may Process Personal Data in ways that are incompatible with the defined purpose or that it will reveal information or make predictions that are not desired, these factors should be taken into account when developing the solution and when choosing the training dataset. The ultimate aim is to try to prevent the undesired result and any unwanted form of Further Processing.

16.3.2 FAIR AND LAWFUL PROCESSING

16.3.2.1 Lawfulness

If Personal Data will be processed within the Artificial Intelligence solution or as part of its training, a legitimate legal basis is required for the Processing to take place. Considering the complexity of Artificial Intelligence systems, finding and justifying an appropriate legal basis can be particularly challenging. Chapter 3 outlines different legal grounds and points out the limitations of using Consent as a legal basis in Humanitarian Action. Adding to those difficulties, limitations to the use of Consent, in particular the possibility of withdraw it, are also relevant to the development and improvement of Artificial Intelligence solutions. Some of the reasons why Consent in Artificial Intelligence may not be considered fully informed or freely given include "long and technical data processing notices, social and

⁴¹⁹ M. Kosinskia, D. Stillwella and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior", *PNAS*, Vol. 110, No. 15, 2013, p. 1: <https://www.pnas.org/content/pnas/early/2013/03/06/1218772110.full.pdf>.

⁴²⁰ Kosinskia, Stillwella and Graepel, 2013, p. 1.

technical lock-ins, obscure interface design, and a lack of awareness on the part of the data subject”.⁴²¹

As mentioned in the introduction to this chapter, the models generated by Artificial Intelligence can be static or dynamic. These two types of model can have different data protection implications. Static models will process Personal Data only to perform the task assigned to the system, while dynamic models will process data to reach the desired output, but also to refine the system in order to provide more accurate results. This means that the purpose and legal basis for Processing data in each model will differ.

If, for instance, a Humanitarian Organization opts for a dynamic model, it should identify an appropriate legal basis to process Personal Data to train the algorithm to achieve a clearly defined purpose. A legal basis should also be defined for the Processing of new Personal Data to fulfil the intended objective once the system has been trained. Lastly, the organization should also identify a legal basis for Processing data to improve the dynamic model.

With dynamic models, including off-the-shelf solutions developed by technology companies, it is important to remember that all data fed into the system during development and application will be used to improve it. This may pose further challenges to the use of Consent, since beneficiaries might agree to having their Personal Data processed for a particular humanitarian purpose, but may not expect it to be used for the development of the Artificial Intelligence solution.⁴²² In such cases, if the identified legal basis for Processing is Consent, the Data Subjects should be informed, in an easy-to-understand manner, of the reasons why their data are requested, what they will be used for, and how they will influence the solution. They should also be informed of potential risks, such as re-identification by the solution (as mentioned in section 3.1) or the fact that their data could be accessed during an attack (as mentioned in the introduction above). That way, organizations can ensure that they obtain fully informed Consent from Data Subjects.

In light of the above, Consent may not always be an appropriate legal basis for the use of Artificial Intelligence in the humanitarian sector. While the delivery of aid or lifesaving services may mean that vital interest⁴²³ or public interest⁴²⁴ can be considered legitimate legal bases to justify the Processing of Personal Data, the development of Artificial Intelligence solutions sometimes may not. To determine whether the improvement of Artificial Intelligence solutions is acceptable under the

⁴²¹ A. Mantelero, A., *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Council of Europe, 2019, p. 7: <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>.

⁴²² Future of Privacy Forum, 2018, p. 8.

⁴²³ See [Section 3.3: Vital interest](#).

⁴²⁴ See [Section 3.4: Important grounds of public interest](#).

chosen legal basis, an organization should consider whether the Further Processing for the improvement of the solution is compatible with the initial purpose for which it collected the Personal Data.

16.3.2.2 Fairness v. bias

The principle of fairness⁴²⁵ requires that all Processing activities respect Data Subjects' interests, and that Data Controllers take action to prevent arbitrary discrimination against individuals.⁴²⁶ The issue of discriminatory bias in Artificial Intelligence is widely recognized and debated.

EXAMPLE:

In a well-known example, an Artificial Intelligence solution was developed in the United States to predict reoffending rates in criminal cases, in order to help judges decide whether or not to grant bail to convicted offenders. The solution incorrectly rated black defendants as being almost twice as likely to reoffend as white defendants.⁴²⁷

To minimize the risk of discriminatory bias, it is recommended that Artificial Intelligence developers “adopt a human rights by-design approach and avoid any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects.”⁴²⁸

Bias in Artificial Intelligence solutions may stem from the use of biased datasets as training data, from systemic biases in society, or even from developers deciding which features to assign more value to in each dataset. Moreover, when there are historical biases in society, it may be difficult to find unbiased data to train the solution. Here, the solution may merely reinforce systemic biases contained in the dataset. Consequently, a model must be trained with relevant and correct data and must also learn which features to emphasize, so as to not assign too much weight to discriminatory aspects that may exist in the data. When there is a risk of arbitrary discrimination, information related to racial or ethnic origin, political opinion, religious and philosophical beliefs, sexual orientation, or any other information that could be grounds for discrimination should not be processed or should be protected so that they are not disproportionately emphasized.⁴²⁹

⁴²⁵ See [Section 2.5.1: The principle of the fairness and lawfulness of Processing](#).

⁴²⁶ The Norwegian Data Protection Authority, 2018, p. 16.

⁴²⁷ J. Angwin *et al.*, “Machine Bias”, ProPublica, 23 May 2016: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

⁴²⁸ CoE, *Guidelines on artificial intelligence and data protection*, 2019, p. 2: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>.

⁴²⁹ The Norwegian Data Protection Authority, 2018, p. 16.

The fact that Artificial Intelligence models should not emphasize such categories of data does not mean, however, that suppressing them from the dataset will necessarily eliminate the risk of bias. The system could correlate other features such as race or gender, and the model may learn to be biased based on those correlated features, which are known in this context as ‘proxies’.⁴³⁰ Moreover, since the main discriminatory feature has been removed from the dataset, it might be more difficult to detect and correct the bias.

EXAMPLE:

A separate study looking at the US predictive solution discussed earlier found that, in almost 70% of cases, the algorithm made a correct reoffending prediction despite its clear bias. In this second study, however, race was not included in the dataset, highlighting “the challenge of finding a model that doesn’t create a proxy for race (or other eliminated factor) – such as poverty, joblessness, and social marginalization.”⁴³¹

For this reason, when choosing the training dataset, an Artificial Intelligence developer – whether acting as an independent Data Controller, a Data Processor, or a joint Controller with a Humanitarian Organization – needs to assess the quality, nature and origin of the Personal Data used, and consider the potential risks to individuals and groups of using de-contextualized data to create de-contextualized models.⁴³² One way to achieve this is for Data Controllers to include, in the continuous DPIA process (see section 2 of this chapter), “frequent assessments on the datasets they process to check for any bias,” and to “develop ways to address any prejudicial elements, including any over-reliance on correlations.”⁴³³ As discussed in section 2 above, not taking such measures has both legal and ethical implications.

16.3.2.3 Transparency

Alongside fairness, transparency is another crucial aspect of data protection. According to this principle, the Processing of Personal Data must be transparent⁴³⁴ for the Data Subjects involved, who should receive at least a minimum amount of information concerning the Processing when their data are collected.⁴³⁵ Transparency, however, can be a challenging principle to apply when it comes to Artificial Intelligence, since these solutions are based on advanced technology that

⁴³⁰ Centre for Information Policy Leadership, 2018, p. 14.

⁴³¹ Future of Privacy Forum, 2018, p. 15.

⁴³² CoE, 2019, p. 2.

⁴³³ EU Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 2018, p. 28: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

⁴³⁴ See [Section 2.5.1: The principle of the fairness and lawfulness of Processing](#).

⁴³⁵ See [Section 2.10: Information](#).

can be hard to understand and explain in lay terms.⁴³⁶ Moreover, many Machine Learning models include multi-layered networks in which the outputs are a result of an internal process that may not be replicated or understood mathematically even by the data scientists and the solution designers themselves.⁴³⁷ This multi-layered architecture is commonly known as the ‘black box’, since it may make it impossible for those using the solution to understand how it reached a specific conclusion or prediction (such as which features were assigned more weight in the process). In other words, the reasoning behind the choice of weight is in most cases not transparent or intelligible for human beings due to Artificial Intelligence’s high degree of complexity. Consequently, it is difficult to assert if the choice of features is comprehensive and if their weightings are reasonable.

One suggested answer to the challenge of transparency in Artificial Intelligence applications is to explain the logic behind the solutions, in other words: “[g]iving information about the type of input data and the expected output, explaining the variables and their weight, or shining light on the analytics architecture”.⁴³⁸ This approach, known as ‘interpretability’, focuses on understanding the causality of a change in the input to the output, without necessarily explaining all the logic of the machine through its multiple layers. In the case of black boxes, however, achieving interpretability will often be difficult and it is important to be transparent with Data Subjects about unknowns and areas of uncertainty.

16.3.3 DATA MINIMIZATION

The data minimization principle requires organizations to limit the Processing of Personal Data to the minimum amount and extent necessary to attain the purpose of the Processing.⁴³⁹ With Artificial Intelligence, however, it may be difficult to know in advance what is necessary,⁴⁴⁰ since these solutions recognize features and patterns by themselves, making it hard to understand what data, and how much, are needed to complete a certain task. Consequently, as techniques such as Machine Learning require large amounts of data to produce useful results, only a certain degree of minimization is possible.⁴⁴¹ Moreover, such solutions must be trained using a suitably large and representative dataset, otherwise they could produce biased results.⁴⁴²

⁴³⁶ The Norwegian Data Protection Authority, 2018), p. 19.

⁴³⁷ Future of Privacy Forum, 2018, p. 17.

⁴³⁸ Mantelero, 2019, p. 12.

⁴³⁹ See [Section 2.5.4: The principle of data minimization](#).

⁴⁴⁰ Centre for Information Policy Leadership, 2018, p. 14.

⁴⁴¹ Mantelero, 2019, p. 8.

⁴⁴² Centre for Information Policy Leadership, 2018, p. 13.

Despite this apparent contradiction between Artificial Intelligence and data minimization, various mitigation measures exist. These are set out below, along with their potential limitations:

- Employing techniques that can make it harder to identify individuals through the data, such as restricting the amount and nature of the information used. This approach may not fit certain Artificial Intelligence solutions that require large amounts of data to function well. In addition, making data hard to identify does not, by itself, guarantee respect for the data minimization principle.
- Using ‘synthetic data’ as training data. Synthetic data “is an artificial data set, including the actual data on no ‘real’ individuals, but which mirrors in characteristics and proportional relationships all the statistical aspects of the original dataset”.⁴⁴³ However, this technique also poses challenges since synthetic data is derived from an original set of real data (which is needed for synthetic data to be able to reflect the society and situation being analysed by the solution to produce accurate results). As such, there is still a risk of re-identification when using synthetic datasets.
- Adopting a progressive approach by collecting what is thought to be the minimum amount of data necessary to achieve the expected results and then testing the solution in order to see how it performs. After testing, more data may be added if needed, and the solution can be tested again until it achieves the desired outcomes. This approach reduces the Processing of unnecessary data and seeks to ensure that the solution is trained on the minimum possible dataset, while also making re-identification harder.

Despite the challenges associated with data minimization in Artificial Intelligence, this principle does not mean that large-scale Processing is forbidden, but rather that it poses higher risks that require appropriate security and risk-mitigation measures. Moreover, as mentioned previously, not all Artificial Intelligence solutions require large volumes of data to be accurate. Those based on reinforcement learning, for instance, can be trained with little or no data.

16.3.4 DATA RETENTION

Personal Data should be retained for a defined period, which should be no longer than is necessary for the purpose of the Processing.⁴⁴⁴ However, once Personal Data is deleted after a certain period of time, it can longer be used to train, deploy or monitor the system, all of which can improve its performance.⁴⁴⁵ If a model shows bias, for example, it can be helpful to have the data available to understand which features were incorrectly weighted and to retrain the solution to provide

⁴⁴³ Future of Privacy Forum, 2018, p. 8.

⁴⁴⁴ See [Section 2.7: Data retention](#).

⁴⁴⁵ Centre for Information Policy Leadership, 2018, p. 15.

more accurate outcomes. Despite the benefits of storing data for longer periods in Artificial Intelligence solutions, Data Controllers must ensure that they retain Personal Data for no longer than is necessary and take measures to ensure that data remains updated throughout the retention period to reduce the risk of inaccuracies in the solution.⁴⁴⁶ Given the variety of uses Artificial Intelligence may have in the humanitarian sector, specific retention periods should be considered in the context of each programme. In this regard, Humanitarian Organizations should consider and set an initial retention period, such as a two-year period for audit purposes. Should the data still be needed after this initial period, organizations should conduct periodic assessments based on their retention needs and consider their legal basis for amending the retention period. They will also need to seek additional Consent from Data Subjects if their data are retained for longer than the duration they consented to at the point of collection.

16.3.5 DATA SECURITY

Data security⁴⁴⁷ is an essential aspect of implementing Artificial Intelligence solutions, particularly in the humanitarian sector. Humanitarian Organizations must be mindful of the risks that these technologies pose and implement the highest level of data security when using them. Attacks by malicious parties typically fall into one of three categories:

- **model inversion attacks:** attempts to reveal information about the training data by inverting the system's model
- **poisoning attacks:** attempts to decrease the utility of the model
- **backdoor attacks:** attempts to gain unauthorized access to the solution and modify it after it has been trained.

Looking specifically at model inversion, it has been demonstrated that some systems remember their training datasets. For example, if a person's face has been used to train a facial recognition system, a malicious party could query the system again and again, slowly changing the input image to reconstruct the face with sufficient precision to know that the person in question was part of the training set.⁴⁴⁸

Another type of deliberate attack involves adding noise to the data in order to decrease the quality of outcomes, sometimes even leading to useless results such as making wrong classifications and predictions.

⁴⁴⁶ EU Article 29 Working Party, 2018, p. 12.

⁴⁴⁷ See [Section 2.8: Data security and Processing security](#).

⁴⁴⁸ M. Fredrikson, S. Jha and T. Ristenpart, "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures" (2015). *CCS '15 Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 1322–1333: <https://www.cs.cmu.edu/~mfredrik/papers/fjr2015ccs.pdf>.

All of these factors mean that inadequate data security can pose significant risks for vulnerable individuals in the context of the use of Artificial Intelligence. In view of these risks, it is important to build strong and secure systems that effectively protect against unauthorized access. Pseudonymization and encryption techniques are some of the methods that can assist in this regard. While the technique of training models on encrypted data is still in its early days, static models that receive encrypted inputs and produce encrypted outputs are already commonplace, albeit with their own constraints. The use of differential privacy⁴⁴⁹ should also be considered when training Artificial Intelligence solutions.

16.4 RIGHTS OF DATA SUBJECTS

Data Controllers are responsible for determining the means and purposes of the Processing and for ensuring that Data Subjects can exercise their rights.⁴⁵⁰ Although Artificial Intelligence may make it more difficult for Data Controllers to comply with these obligations, choosing such solutions as a means to achieve a certain purpose does not excuse Data Controllers from their responsibilities. Humanitarian Organizations should therefore have procedures and systems in place to ensure that individuals can exercise their rights. They should also employ the principles of data protection by design and by default (see section 7 below). At the same time, as is discussed in section 2.11 of this Handbook, the exercise of these rights may be limited in certain circumstances.

16.4.1 RIGHT TO BE INFORMED

As with other technologies, when Artificial Intelligence is applied, Data Subjects should be informed⁴⁵¹ of the identity and contact details of the Data Controller, how the controller can be contacted, the purpose and legal basis of the Processing, the categories of Personal Data that are being processed, their rights as Data Subjects (especially the right of access), and safeguards connected with the Processing. Additionally, Data Subjects should be informed about the use of Artificial Intelligence, its significance for the envisaged Processing, and the risks, rules and safeguards connected with the Processing.⁴⁵²

⁴⁴⁹ “Differentially-private algorithms are resilient to adaptive attacks that use auxiliary information. These algorithms rely on incorporating random noise into the mix so that everything an adversary receives becomes noisy and imprecise, and so it is much more difficult to breach privacy (if it is feasible at all).” A. Elamurugaiyan, “A Brief Introduction to Differential Privacy”, Medium, 31 August 2018: <https://medium.com/georgian-impact-blog/a-brief-introduction-to-differential-privacy-eacf8722283b>.

⁴⁵⁰ See [Section 2.11: Rights of Data Subjects](#).

⁴⁵¹ See [Section 2.10: Information](#).

⁴⁵² The Norwegian Data Protection Authority, 2018, p. 19.

16.4.2 RIGHT TO ERASURE

Organizations should give due consideration to the right to erasure when using Artificial Intelligence solutions.⁴⁵³ If a Data Subject requests that their data be deleted, but such data have been used to train a specific solution, the solution will still be based on the data even if they can be deleted. This means that, even if the Humanitarian Organization deletes the data from the dataset, the solution may still contain certain features of the data (because their features were analyzed and compared to others in the dataset to create the solution). This can be a problem when, as outlined above, the original data can be revealed through a model inversion attack.

In this case, it is important to consider whether deleting the datasets themselves without altering the solution would constitute a limitation to the right to erasure and, if so, whether such limitation would be justified in the circumstances. Regardless of the challenges related to erasure, “[t]he right to object should be ensured in relation to processing based on technologies that influence the opinions and personal development of individuals.”⁴⁵⁴ Importantly, however, there may be valid reasons to limit this right, as discussed in section 2.11 of this Handbook.

16.4.3 RIGHTS IN RELATION TO AUTOMATED DECISION-MAKING

Data Subjects have the right to not be subjected to solely automated decision-making, i.e. “decisions by technological means without human involvement,”⁴⁵⁵ when such decisions produce legal effects or similarly significantly affect the individual in question.

EXAMPLE:

Some examples of solely automated decision-making include speeding fines imposed purely on the basis of evidence from speed cameras, automatic refusal of an online credit application, or e-recruiting practices without any human intervention.⁴⁵⁶

The rationale behind this right “is driven by a concern for algorithmic bias; a worry of incorrect or unsubstantiated solely automated decisions based on inaccurate or incomplete data; and the need for individuals to have redress and the ability to contest a decision if an algorithm is incorrect or unfair.”⁴⁵⁷ These concerns are justified by examples such as the Swedish benefits case mentioned above, where a rogue solution meant that “thousands of unemployed people were wrongly denied

⁴⁵³ See [Section 2.11.4: Right to erasure](#).

⁴⁵⁴ CoE, 2019, p. 2.

⁴⁵⁵ CoE, 2019, p. 8.

⁴⁵⁶ CoE, 2019, p. 8.

⁴⁵⁷ Centre for Information Policy Leadership, 2018, p. 16.

benefits.”⁴⁵⁸ In Humanitarian Action, a similar problem could arise if Artificial Intelligence solutions make decisions about who receives aid or who is included in a target population for an aid programme. Beneficiaries should always have the right to have a human being oversee decisions that affect them.

It should be noted that “[t]o qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture.”⁴⁵⁹ This is particularly important because those making decisions may blindly rely on the Artificial Intelligence solution’s suggestions on the basis that mathematical algorithms are supposedly failproof. Consequently, the presence of an individual human decision-maker alone is not sufficient.⁴⁶⁰ The decision-maker must have the ability to refute the machine’s decision or suggestion.

On a similar note, decision-makers may not fully understand how the system arrived at a particular decision or suggestion and may therefore find it difficult to assess whether it was made wrongly (see Section 3.2.3 on transparency above). Decision-makers should always be able to examine all the facts and information from scratch and make an independent decision, without considering the Artificial Intelligence solution’s outcome. This is not always straightforward, however, since an Artificial Intelligence solution is able to process much more information than a person in the same situation. Setting up a multi-disciplinary team, including individuals with expertise in the sector and technology developers, may be one option in such cases.

It is possible that individuals, regardless of their level of expertise, may be reluctant to challenge an Artificial Intelligence’s automated decisions, given how accurate the technology can be. Consequently, another issue to take into account is how the human intervention would be arranged so that a review of the decision is “carried out by someone who has the appropriate authority and capability to change the decision.”⁴⁶¹ Organizations therefore need to consider whether it would be acceptable for beneficiaries to be subjected to automated decision-making if they had the right to request human intervention. Here, the very case for using the technology in the first place may come under challenge.

In any case, it is essential that beneficiaries are informed about any automated decision-making they are being subjected to, including the logic behind the Artificial Intelligence solution, the significance of the Processing, and its envisaged consequences for them.⁴⁶² They must also be able to object to the Processing.

⁴⁵⁸ Wills, 2019.

⁴⁵⁹ EU Article 29 Working Party, 2018, p. 21.

⁴⁶⁰ Mantelero, 2019, p. 11.

⁴⁶¹ EU Article 29 Working Party, 2018, p. 27.

⁴⁶² EU Article 29 Working Party, 2018, p. 25.

16.5 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

16.5.1 ACCOUNTABILITY

As explained above, Artificial Intelligence sometimes evolves in ways that cannot be fully understood by developers due to the ‘black box’ effect (see section 4.2.3). This may raise questions around the principles of accountability and responsibility of the Data Controller. To implement these principles, Data Controllers need to comply with data protection requirements and be in a position to demonstrate that they have taken adequate and proportionate technical and organizational measures within their respective Processing operations.⁴⁶³

16.5.2 LIABILITY

Automated decision-making (see above) raises particular issues around liability. In health care, for instance, machines are often considered to be more accurate than humans at diagnosing diseases such as specific types of cancer, or at analysing X-ray images. For this reason, doctors may feel compelled to follow the machine’s recommendation.⁴⁶⁴ Here, it might be unclear who is responsible for the diagnosis – the machine itself (assuming it should be considered a legal entity), its developers, or the doctor.⁴⁶⁵ A similar situation could also occur where a Humanitarian Organization offers medical services in an emergency – for instance, if someone is misdiagnosed during a contagious disease outbreak. To counterbalance this, organizations may seek to extend the product liability logic to algorithms, thereby placing the full burden of liability on the developer company⁴⁶⁶ (although this may be very difficult to negotiate in practice). From an ethical perspective, it is also important for Humanitarian Organizations to understand their own responsibilities when choosing to use such technology and to be accountable to beneficiaries accordingly.

⁴⁶³ See [Section 2.9: The principle of accountability](#).

⁴⁶⁴ French Data Protection Authority (CNIL), “Comment permettre à l’homme de garder la main? Les enjeux éthiques des algorithmes et de l’intelligence artificielle”, 2017, p. 27: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.

⁴⁶⁵ CNIL, 2017, p. 27.

⁴⁶⁶ Mantelero, 2019, p. 17.

16.6 INTERNATIONAL DATA SHARING

Personal Data and other types of data processed in Artificial Intelligence solutions will routinely flow across national borders. This raises questions about data protection in Artificial Intelligence applications when data are shared internationally.⁴⁶⁷ Although recognized legal mechanisms exist, they may be all-but impracticable in an Artificial Intelligence context.

Determining applicable law and jurisdiction can also present challenges. The proper and targeted risk analysis necessary for transfers is impossible unless choice of jurisdiction and choice of law are clearly embedded in Artificial Intelligence governance. The principles described in section 4.2 of this Handbook provide more in-depth guidance to Humanitarian Organizations on international data sharing in the context of Artificial Intelligence. Accountability for data sharing is a key principle to consider when organizations engage in activities that involve International Data Sharing.

16.7 DATA PROTECTION BY DESIGN AND BY DEFAULT

Data Protection by design and by default involves designing a Processing operation, programme or solution in a way that implements key data protection principles from the outset, and that provides the Data Subject with the greatest possible data protections. The key data protection principles in this sense are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation (limited retention)
- integrity and confidentiality (security)
- accountability.

Refer to Chapter 2 of this Handbook for a general description of these principles, some of which are covered in section 3 above.

Certain characteristics of Artificial Intelligence can pose challenges to the implementation of data protection-compliant solutions, as explained in section 3 above. Building solutions in a way that seeks to address these challenges and risks from the outset may be one of the most effective ways to avoid or mitigate them. For instance, most Artificial Intelligence technologies operate by processing large volumes of data to learn how to weigh their relevant features, identify patterns, and train models to improve themselves. Such data are rarely anonymized, since

⁴⁶⁷ See [Chapter 4: International Data Sharing](#).

Artificial Intelligence often requires detailed datasets to work properly. However, the more unique features that are added to datasets, the higher the chances that they will identify the person to whom the data relate – either because the model makes more inferences than initially intended (see section 3.1), or because the system comes under deliberate attack (see section 3.5). Ultimately, decisions on whether or not to use Artificial Intelligence technologies will always involve weighing their potential benefits against their possible risks to Data Subjects.

Synthetic data (see above) is frequently suggested as a possible solution to re-identification. But it is not bulletproof because synthetic data are derived from an original set of real data, and if numerous unique features remain from the original dataset, re-identification problems may still rise. The possibility of re-identifying beneficiaries from the model is also particularly relevant in the humanitarian sector, where ill-intentioned individuals or organizations may wish to obtain the data the Humanitarian Organizations collects to target or harm vulnerable people or groups. Pseudonymization, Anonymization (where possible) and encryption techniques can also help to avoid re-identification and protect the identity of Data Subjects.⁴⁶⁸ Combining encryption with pseudonymization or the use of synthetic data adds an extra layer of protection. This is because attackers who gain access to the system will not be able to ‘read’ any information they obtain without the decryption key.

The training data must also be fit for the purpose of the Artificial Intelligence solution. In other words, the selected data must be relevant to the task, and constant checks and updates will be required to identify inaccurate and/or corrupt data and remove them from the training dataset. New data may also be added to avoid bias (see section 3.2.2). It is therefore important that Humanitarian Organizations work with developers to ensure the solution they acquire or develop will be applicable or suited to the organization’s needs in a particular context.

Humanitarian Organizations will also need to work with developers on the issue of “explainability”, especially when they intend to use Artificial Intelligence solutions to support decision-making. They should be able to explain to Data Subjects how the solution works, what risks that may emerge, how the Artificial Intelligence system reaches its outcomes, and what arrangements are in place for a human decision-maker to review its decisions or suggestions if needed.

In conclusion, when choosing to deploy Artificial Intelligence solutions, Humanitarian Organizations are encouraged to invest in data protection by design as an essential part of the development or procurement process. This is likely to be the most effective way to ensure compliance with data protection principles.

⁴⁶⁸ The Norwegian Data Protection Authority, 2018, p. 18.

16.8 ETHICAL ISSUES AND CHALLENGES

Given the speed at which technologies are evolving and the fact that the law typically lags behind major societal changes, it is likely that some of the ethical issues associated with Artificial Intelligence solutions are not yet covered by existing laws. When opting to develop or use such a solution, Humanitarian Organizations should of course consider whether it complies with data protection laws and data protection by design principles. Importantly, however, they should also reflect on its potential adverse impacts on a variety of Data Subjects' fundamental rights, and on the ethical and social implications of the data Processing.⁴⁶⁹

Artificial Intelligence tools present many risks, such as the possibility of discriminatory bias, difficulty in establishing liability, system accuracy, and possible privacy infringements. Also, some developers may train systems on data obtained either illegally or through unethical methods, such as only allowing access to their platform or services if users consent to their data being used to train Artificial Intelligence. This is particularly worrisome when users of such platforms or services are members of vulnerable groups and need to consent to access services without the company being transparent about the data they Process. Ethical deployment of Artificial Intelligence will always involve ensuring that the data used were collected in accordance with accepted human rights standards, and that specific personal and/or group identifiers have been pseudonymized.

Risk assessments that go beyond traditional data protection and cover a wider range of interests, ethical standards and rights (such as the right to non-discrimination)⁴⁷⁰ are of great importance. Societal interests and ethics are broader than law, and organizations should consider the wider contextual background, including political and cultural nuances. This makes evaluating ethical values more complex, context-dependent and comprehensive than assessing compliance with data protection laws alone.

There have been numerous attempts to define the ethical principles that apply to the development of Artificial Intelligence. Examples include the Asilomar AI Principles⁴⁷¹ and the International Conference of Data Protection and Privacy Commissioners' Declaration on Ethics and Data Protection in Artificial Intelligence.⁴⁷² Academics are

⁴⁶⁹ A. Mantelero, "Artificial Intelligence and Big Data: A blueprint for a human rights, social and ethical impact assessment", *Computer Law & Security Review*, Vol. 34, Issue 4, 2018, p. 755: <https://doi.org/10.1016/j.clsr.2018.05.017>.

⁴⁷⁰ Mantelero, 2019, p. 13.

⁴⁷¹ Future of Life Institute, "Asilomar AI Principles": <https://futureoflife.org/ai-principles/>.

⁴⁷² International Conference of Data Protection and Privacy Commissioners, "Declaration on Ethics and Data Protection in Artificial Intelligence": http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf?mc_phishing_protection_id=28047-br1tehqdu81eaoar3q10.

also conducting research into ethical issues related to Artificial Intelligence,⁴⁷³ and some multinational companies are developing their own sets of ethical principles. Although there is currently no harmonization across these initiatives, and no single set of standard guidelines, principles that span both ethics and law – such as transparency, fairness and accountability (see Section 3 above) – seem to provide a common ground.

Given the impact Artificial Intelligence can have, “ethics committee is attracting increasing attention in AI [Artificial Intelligence] circles”⁴⁷⁴ as they “can provide valuable support to developers in designing rights-based and socially-oriented algorithms”.⁴⁷⁵ In terms of the composition of such committees, “[w]here societal issues are significant, legal, ethical or sociological expertise, as well as domain-specific knowledge, will be essential”.⁴⁷⁶ Humanitarian Organizations could therefore consider establishing an ethics committee to assist them in dealing with such issues when deploying Artificial Intelligence solutions.

To ensure compliance with legal and ethical standards, Humanitarian Organizations should consider the following two steps:

- First, they should answer the following three questions during their DPIA process:
 - What should actually be done?
 - What is legally allowed?
 - What is technically possible?
- Second, when choosing to use new technologies, they should consider the problem they are facing and whether Artificial Intelligence can help solve it by asking the questions below:
 - What problem is solved with Artificial Intelligence?
 - What problem is not solved?
 - What problem is created?
 - How does this technology perform compared with other technologies that may be less risky?

The zero option (not using Artificial Intelligence) should also always be kept in mind. This is particularly relevant where the use of Artificial Intelligence would be legal but not ethically acceptable. For instance, if the solution chosen by the organization is not well accepted by programme’s intended beneficiaries, this feeling of discomfort or mistrust may justify a decision not to deploy the technology.

⁴⁷³ See, for example the ACM conference on Fairness, Accountability and Transparency (<https://fatconference.org>), which has gained prominence in recent years.

⁴⁷⁴ Mantelero, 2019, p. 15.

⁴⁷⁵ Mantelero, 2019, p. 16.

⁴⁷⁶ Mantelero, 2019, p. 16.

APPENDIX I

TEMPLATE FOR A DPIA REPORT

Cover page

- Data Protection Impact Assessment on [name of activity]
- Contact person, title and email address
- Date

Executive summary

If the DPIA is more than 20 pages, it should include an executive summary. The executive summary should include details of why the DPIA was undertaken, for whom and who conducted it. The executive summary should include the key findings and principal recommendations.

Introduction and overview of the DPIA process

The introduction should outline the scope of the DPIA, when, why and for whom it was performed and by whom. It should provide some information about the activity assessed. It should introduce the methodology employed in the DPIA (e.g. the method chosen to engage stakeholders).

Threshold assessment

This section should list the questions addressed by the Humanitarian Organization to determine whether a DPIA was necessary and what should be the scale of the DPIA.

Description of the activity or project to be assessed

The description of the activity to be assessed should state who is undertaking the activity and when it is to be undertaken. It should state who will be affected by the activity, who might be interested in or affected by the activity. The description should provide contextual information about how the activity fits in with the Humanitarian Organization's other services or activities.

Information flows

This section should detail (at a minimum):

- the type of data to be collected
- whether sensitive information will be collected
- how the data will be collected
- for what purposes the data will be used
- how and where the data will be stored and/or backed up
- who will have access to the Personal Data
- whether Personal Data will be disclosed
- whether sensitive Personal Data will be disclosed
- whether any data will be transferred to other organizations or countries.

Compliance with laws, regulations, codes and guidelines

The DPIA report should identify the laws, regulations, codes of conduct and guidelines with which the activity complies or should comply. At the global level, the privacy principles listed in the ISO/IEC 29100:2011 standard of the International Organization for Standardization (ISO)⁴⁷⁷ are useful as a reference in a DPIA. In addition, the DPIA report should state how it complies with the Humanitarian Organization's confidentiality rules and codes of conduct, and how the Humanitarian Organization monitors compliance.

Stakeholder analysis

The report should identify who are the principal stakeholders interested in or affected by the data Processing and how the DPIA or the Humanitarian Organization arrived at this list.

Data protection impacts (risks)

This section should detail the privacy risks identified in relation to the main privacy principles found in relevant legislation and the Humanitarian Organization's confidentiality rules and codes of conduct.

Risk assessment

This section of the report should include details of how the risks were assessed and the results of any risk assessment undertaken.

Organizational issues

The DPIA report should include a section that describes how senior management is involved in decision-making related to data protection. This should include discussion identifying any organizational issues that are directly or indirectly affected by the data Processing activity. For example, it may become apparent that the data Processing requires putting in place an organizational mechanism for ensuring accountability, i.e. that a senior manager is responsible for ensuring that the programme does not negatively affect the Humanitarian Organization or its stakeholders.

In the course of the DPIA, it may become apparent to the DPIA team that the Humanitarian Organization needs to spend more time on raising the awareness of employees about privacy and/or ethical issues, and that the Humanitarian Organization needs to mainstream data protection in the organization. The report should state what the Humanitarian Organization does now to raise employee awareness of data protection and how it could improve.

⁴⁷⁷ <https://www.iso.org/standard/45123.html>.

The report should state how the Humanitarian Organization identifies, investigates and responds to data protection incidents, e.g. data protection breaches, how the Humanitarian Organization decides to notify affected parties and how it seeks to learn from an incident.

This section should also describe how the Humanitarian Organization responds to requests for access to personal information or to correct or amend the information it has gathered and to whom the data are transferred and what safeguards the Humanitarian Organization insists be in place before making a transfer.

Results of the consultation(s)

The report should specify what efforts the Humanitarian Organization has made to consult with stakeholders, to gather their views and ideas about potential data protection impacts, how they might be affected by the data Processing (positively and/or negatively) and how negative impacts could be mitigated, avoided, minimized, eliminated, transferred or accepted.

The DPIA team should specify which consultation techniques were employed (surveys, interviews, focus groups, workshops, etc.), when they were undertaken, the results of each consultation exercise, and whether differences in opinion were discovered when different techniques were used.

The DPIA should state who was consulted and what information materials the Humanitarian Organization provided to stakeholders, including families of the missing.

The DPIA should state whether the consultations yielded any new findings and what efforts the Humanitarian Organization had made to take into account stakeholder views and ideas in the design of the data Processing activity.

Recommendations

The DPIA team should set out their recommendations for avoiding, minimizing, transferring or sharing the data protection risks. Some risks may be worth taking and, if so, the DPIA should say why. The DPIA should be clear who will bear the risk (i.e. will it be the Humanitarian Organization or stakeholders or others?). The DPIA should also set out what further work is necessary or desirable to implement its recommendations (for example, the DPIA should mention the need for independent third-party monitoring of its recommendations).

The DPIA should also make recommendations as to whether the DPIA report should be made public. There may be circumstances where it might not be appropriate to make the DPIA or parts of it public – e.g. there may be confidentiality or security reasons. Often the report can be redacted in places and then made public or sensitive parts can be placed in a confidential appendix. Alternatively, the Humanitarian Organization could provide a summary of the DPIA report.

APPENDIX II


WORKSHOP PARTICIPANTS

All workshops were co-organized by the Brussels Privacy Hub and the ICRC. Workshop participants included representatives of the following organizations:

- Barclays
- Belgian Privacy Commission
- Biometrics Institute
- Brussels Privacy Hub
- Canadian Red Cross
- Cash Learning
- Council of Europe
- Council of the EU
- Dalberg Data Insights
- EFTA Surveillance Authority
- Engine Room
- European Commission, DG ECHO
- European Commission, DG Justice
- European Data Protection Supervisor
- European UAV-Drones Area
- Facebook
- Fairphone
- French-speaking Association of Personal Data Protection Authorities
- French Data Protection Authority
- Government of Luxembourg
- GSMA
- Harvard Humanitarian Initiative
- Human Rights Watch
- ID2020
- International Committee of the Red Cross
- International Federation of the Red Cross
- International Organization for Migration
- ITU
- KU Leuven
- MasterCard
- Médecins Sans Frontières
- Mercy Corps
- Microsoft
- MIT
- Netherlands Red Cross
- Norwegian Red Cross
- Orange Business Services
- Oxford University
- Politecnico di Torino
- Privacy International
- Queen Mary University of London
- Royal Military Academy Belgium

- Ryerson University – Privacy by Design Centre of Excellence
- Sensometrix
- SES
- Spanish Data Protection Agency
- Swiss Data Protection Authority
- Swiss Federal Institute of Technology in Lausanne
- UN Global Pulse
- UN Office of the Special Rapporteur on the Right to Privacy
- United Nations High Commissioner for Refugees
- United Nations Office for the Coordination of Humanitarian Affairs
- University of Geneva
- USAID
- VIVES University College
- Vrije Universiteit Brussel
- World Food Programme
- World Vision International
- Yale University.

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles.

 facebook.com/icrc

 twitter.com/icrc

 instagram.com/icrc



ICRC

International Committee of the Red Cross
19 avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org
© ICRC, May 2020

ISBN 978-2-940396-80-1

