



Universiteit Leiden



Grotius Centre
for International
Legal Studies



KGF

KALSHOVEN-GIESKES FORUM
ON INTERNATIONAL HUMANITARIAN LAW

TOWARDS A RESPONSIBLE APPROACH TO DATA

Leiden IHL Clinic Report-Series No. 30 (2018)

Written by:

Marta Albaladejo Carreño

Aude Jolliet

Charlotte Vercaeye

Emily Wood

Supervised by:

Dr Emma Irving

Nicholas Ortiz, LL.M.

General coordination by:

Dr Robert Heinsch

June 2018

TOWARDS A RESPONSIBLE APPROACH TO DATA

Report



**Universiteit
Leiden**
The Netherlands



OAM CONSULT

OAM Consult, established by Olivier Mukarji, is a consulting firm based in Copenhagen, Denmark. OAM Consult seeks to harness the power of public and private partnerships for achieving the Sustainable Development Goals. OAM Consult's advisory services target policy, practice and research stakeholders involved in designing and implementing initiatives in three mutually reinforcing areas: Public Private Partnership; Conflict Prevention and Response in the Human Rights, Humanitarian, Development and Peace Nexus (HDPN); Monitoring, Evaluation and Cross Institutional Learning.

Marta Albaladejo Carreño
Aude Jolliet
Charlotte Vercraeye
Emily Wood

The authors would like to thank, in particular, Dr Emma Irving and Nicholas Ortiz for their continuous support, guidance and comments, without which this report would not have been possible.

In addition, the authors would like to thank Olivier Mukarji, Graham Carrington, Iona Eberle, Jane Møller Larsen, Marcus Anderbrandt and Lena Vogel of OAM Consult (our Cooperation Partner) for peer reviewing this report.

The authors would also like to thank the Centre for Innovation, in particular, Thomas Baar and Josje Spierings, for providing training seminars and for organising the Launch Event for this report.

Abstract

To fully harness the opportunities that data offer in the digital age, humanitarian, human rights and development organizations should adopt a responsible approach to data, one that mitigates the risks of harm inherent therein. Yet, there is a noticeable difficulty in implementing such a responsible approach to data, particularly because of the lack of awareness of what such an approach entails and, more importantly, how it can be implemented in practice.

Against this backdrop, the present report aims to provide guidance for organizations working with data and seeking to process data in a responsible manner, or to help them to improve their pre-existing policies. To this end, this report relies on a comparative analysis of the current regulatory data protection frameworks, as well as guidelines developed by humanitarian, human rights and development organizations.

This comparative analysis enables the report to identify the core components of a responsible approach to data. These core components are divided into two categories. Firstly, the entitlements of data subjects (the individuals concerned by the data processing) to privacy, information, access, correction, erasure, objection and participation (discussed in chapter 3). Secondly, a set of data protection principles, relating to legitimate processing, informed consent, purpose limitation, data minimisation, storage limitation, data quality, transparency and openness, data security and accountability (discussed in chapter 4). This comparative analysis is relied upon to define, and explain the scope and content of, each of these core components, and to provide guidance as to how to implement them in practice.

When brought together, these regulatory frameworks and guidelines offer an invaluable set of considerations, as well as practical measures and mechanisms by which to responsibly process data. This collective effort constitutes solid guidance for organizations working with data and seeking to process it in a responsible manner.

While the present report provides a comprehensive overview of the current state of the art of responsible data processing, the development of a responsible approach to data remains a work in progress. This is reflected in this report by way of a description of the fragmented existing ‘regulatory’ landscape concerning data protection (discussed in chapter 2), and of some remaining challenges regarding data protection (discussed in chapter 5).

TABLE OF CONTENTS

Table of Abbreviations.....	1
Glossary of Terms	2
1. INTRODUCTION	4
1.1. Aim of the Report.....	6
1.2. Research Approach	7
1.2.1. Reliance on Frameworks and Guidelines.....	7
1.2.2. Rationale of the Selection of Frameworks and Guidelines.....	9
1.2.3. Comparative Analysis.....	10
1.3. Limitations of the Report.....	11
1.4. Structure of the Report	12
2. THE EXISTING REGULATORY LANDSCAPE	12
2.1. The National Level.....	13
2.2. The Regional Level.....	15
2.3. The International Level.....	17
2.4. Concluding Remarks	18
Table 1: Entitlements and Principles Identified in Regulatory Frameworks	20
Table 2: Entitlements and Principles Identified in Guidelines	21
3. ENTITLEMENTS OF DATA SUBJECTS	22
3.1. Introduction	22
3.2. Privacy	24
3.2.1. Definition.....	24
3.2.2. The Entitlement in Practice.....	24
3.3. Information	27
3.3.1. Definition.....	27
3.3.2. The Entitlement in Practice.....	28
3.4. Access	29
3.4.1. Definition.....	29
3.4.2. The Entitlement in Practice.....	29
3.5. Correction	31
3.5.1. Definition.....	31
3.5.2. The Entitlement in Practice.....	31
3.6. Erasure.....	33
3.6.1. Definition.....	33

3.6.2. The Entitlement in Practice.....	33
3.7. Objection	34
3.7.1. Definition.....	34
3.7.2. The Entitlement in Practice.....	34
3.8. Participation.....	35
3.8.1. Definition.....	35
3.8.2. The Entitlement in Practice.....	35
3.9. Concluding Remarks.....	38
4. DATA PROTECTION PRINCIPLES.....	39
4.1. Introduction	39
4.2. Legitimate Processing.....	40
4.2.1. Definition.....	40
4.2.2. Substance	40
4.2.3. The Principle in Practice.....	42
4.3. Informed Consent	42
4.3.1. Definition.....	42
4.3.2. Substance	42
4.3.3. The Principle in Practice.....	44
4.4. Purpose Limitation	46
4.4.1. Definition.....	46
4.4.2. Substance	46
4.4.3. The Principle in Practice.....	48
4.5. Data Minimisation.....	49
4.5.1. Definition.....	49
4.5.2. Substance	49
4.5.3. The Principle in Practice.....	50
4.6. Storage Limitation	51
4.6.1. Definition.....	51
4.6.2. Substance	51
4.6.3. The Principle in Practice.....	52
4.7. Data Quality	53
4.7.1. Definition.....	53
4.7.2. Substance	53
4.7.3. The Principle in Practice.....	55
4.8. Transparency and Openness	56

4.8.1. Definition.....	56
4.8.2. Substance	56
4.8.3. The Principle in Practice.....	56
4.9. Data Security.....	57
4.9.1. Definition.....	57
4.9.2. Substance	57
4.9.3. The Principle in Practice.....	58
4.10. Accountability	60
4.10.1. Definition.....	60
4.10.2. Substance	60
4.10.3. The Principle in Practice.....	60
4.11. Concluding Remarks	64
5. CONCLUSIONS	65
5.1. Observations: Remaining Challenges.....	65
5.1.1. Risks Emanating from Demographically or Community Identifiable Information.....	65
5.1.2. The Practical Implementation of Entitlements of Data Subjects	66
5.1.3. The Way Forward: Transparency as Part of the Solution?	67
5.2. Final Remarks.....	68
Annex 1: Entitlements of Data Subjects	70
Annex 2: Data Protection Principles.....	71
Table of Cases.....	72
Table of International Legislation	72
Table of Regional Legislation	72
Table of Resolutions of Regional Organizations and Documents of Regional Bodies	73
Guidelines of Humanitarian, Human Rights and Development Organizations Studied	73
Bibliography	74
Books	74
Book Articles.....	75
Journal Articles	75
Online Journals	76
Conference Papers.....	76
Publications of Organizations (other than those studied).....	76
News Articles	78
Websites.....	79

Table of Abbreviations

APEC: Asia-Pacific Economic Cooperation

AU: African Union

CII: Community Identifiable Information

CoE: Council of Europe

DII: Demographically Identifiable Information

DPIA: Data Protection Impact Assessment

DPO: Data Protection Officer

DSA: Data Sharing Agreement

ECHR: European Convention on Human Rights

ECOWAS: Economic Community of West African States

ECtHR: European Court of Human Rights

EU: European Union

GDPR: European Union General Data Protection Regulation

GI-ESCR: Global Initiative for Economic, Social and Cultural Rights

HHI: Harvard Humanitarian Initiative

ICCPR: International Covenant on Civil and Political Rights

ICO: United Kingdom Information Commissioner's Office

ICRC: International Committee of the Red Cross

IFRC: International Federation of the Red Cross and Red Crescent Societies

IO: International Organization

IOM: International Organization for Migration

MSF: Médecins Sans Frontières

NGO: Non-Governmental Organization

NHRI: National Human Rights Institution

OAS: Organization of American States

OCHA: United Nations Office for the Coordination of Humanitarian Affairs

OECD: Organisation for Economic Co-operation and Development

OHCHR: Office of the High Commissioner for Human Rights

PII: Personally Identifiable Information

SSP: Satellite Sentinel Project

UNDG: United Nations Development Group

UNHCR: United Nations High Commissioner for Refugees

UNICEF: United Nations Children's Fund

USAID: United States Agency for International Development

WFP: World Food Programme

Glossary of Terms

Beneficiary: any person who receives assistance or benefits from a project of an organization (particularly humanitarian, human rights and development organizations).¹

Biometric Data: data relating to unique physical, psychological or behavioural characteristics that has been recorded and can be authenticated digitally to identify an individual. Examples include iris and finger print scans, and facial recognition.²

Crowdsourcing: the practice of obtaining data, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional sources.³

Data: raw facts related to any person or thing that exists in the world which may take the form of words, text, numbers, sounds, maps, pictures or videos.

Data Analytics: the practice of combining very large volumes of diversely sourced information (big data) and analysing them, using sophisticated algorithms to inform decisions.⁴

Data Controller: the primary custodian of personal data. This may be an organization or an individual. The data controller determines the purposes for which, and the manner in which, personal data are processed. They retain ultimate responsibility for protection of the data even if they delegate use of the data to other organizations or individuals.⁵

Data Lifecycle: the sequence of stages that a particular unit of data goes through, from collection to its eventual archival or destruction at the end of its useful life.⁶

Data Processing: any operation or set of operations that is performed, either manually or by automated means, on personal data or sets of personal data. Processing includes data collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment and erasure or destruction.⁷

Data Processor: the person or organization who processes personal data on behalf of the data controller.⁸

Data Protection Impact Assessment (DPIA): an assessment that identifies, evaluates and addresses the risks to personal data arising from a project, policy, programme or other initiative.⁹

Data Protection: the systematic application of a set of institutional, technical and physical safeguards that protect data and preserve privacy throughout the entire data lifecycle.¹⁰

¹ Adapted from IOM, 'IOM Data Protection Manual' (IOM 2010) <https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf> accessed 9 June 2018 (IOM) 109.

² WFP, 'WFP Guide to Personal Data Protection and Privacy' (WFP 2016) <<https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/>> accessed 9 June 2018 (WFP) 4.

³ 'Crowdsourcing' (Merriam-Webster, 28 May 2018) <<https://www.merriam-webster.com/dictionary/crowdsourcing>> accessed 22 June 2018.

⁴ Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action* (International Committee of the Red Cross 2017) <<https://shop.icrc.org/icrc/pdf/view/id/2592>> accessed 21 June 2018 (ICRC Handbook) 8.

⁵ WFP (n 4) 4.

⁶ Adapted from Margaret Rouse, 'Definition: Data Life Cycle' (WhatIs, July 2017) <<https://whatis.techtarget.com/definition/data-life-cycle>> accessed 22 June 2018.

⁷ ICRC Handbook (n 4) 9.

⁸ *ibid*, 8.

⁹ *ibid*.

¹⁰ Adapted from IOM (n 1) 110.

Data Subject: a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to personal data.¹¹

Dataset: a collection of separate sets of data that is treated as a single unit by a computer.¹²

Demographically (or Community) Identifiable Information (DII/CII): either individual and/or aggregated data that allows inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age health, condition, location, occupation, and/or other demographically defining factors.¹³

Donor: any person or entity, often a country, which contributes to the funding of an organization's (particularly humanitarian, human rights and development organizations) project.¹⁴

Drones: 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).¹⁵

Further Processing: additional processing of personal data that goes beyond the purposes originally specified at the time the data were collected.¹⁶

Personal Data: any information relating to an identified or identifiable natural person.¹⁷

Personally Identifiable Information (PII): any data that directly or indirectly identifies, or can be used to identify, a data subject. Including, but not limited to, the person's name, address, identification number, gender, age or date of birth, financial accounts numbers, etc.¹⁸

Regulatory Frameworks: data protection instruments at the regional and international level.

Responsible Data: the duty to ensure individual consent, privacy, security and ownership around the data processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness.¹⁹

Sensitive Data: 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.²⁰

¹¹ ICRC Handbook (n 4) 8.

¹² Adapted from 'Dataset' (*Cambridge Dictionary*) <<https://dictionary.cambridge.org/fr/dictionnaire/anglais/dataset>> accessed 22 June 2018.

¹³ Adapted from Daniel Gilman, 'Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies' (Matthew Easton ed, OCHA Policy and Studies Series, OCHA 2014) <www.unocha.org/sites/unocha/files/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf> accessed 22 June 2018 (OCHA Humanitarianism in the Age of Cyber-Warfare) 3.

¹⁴ Adapted from IOM (n 1) 110.

¹⁵ ICRC Handbook (n 4) 8.

¹⁶ *ibid.*

¹⁷ *ibid.*, 9.

¹⁸ Adapted from OCHA Humanitarianism in the Age of Cyber (n 13) 3.

¹⁹ Adapted from Responsible Data Forum, 'The Handbook of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment' (The Engine Room Responsible Data Program 2016) <<https://responsibledata.io/2016/04/13/the-release-of-the-hand-book-of-the-modern-development-specialist/>> accessed 21 June 2018 (Responsible Data Forum) 16.

²⁰ ICRC Handbook (n 4) 9.

1. INTRODUCTION

Data has been described as the “lifeblood of decision making”.²¹ This is because there cannot be an informed decision without information, and there cannot be information without data. Data are raw facts related to any person or thing that exists in the world. Data may take the form of words, text, numbers, sounds, maps, pictures or videos. Only when these data are made sense of, either mentally or with the help of electronic devices, can information be generated. Thus, any individual or organization seeking to obtain information that is not already otherwise available will need to process data. Data processing encompasses any operation, or set of operations, that are performed on data (for example, collection, analysis, storage or sharing).

Data are processed for a variety of reasons, and are also relied upon by actors such as organizations and governments to make informed decisions in areas such as humanitarian action, human rights reporting, development work, and beyond. For example, in a humanitarian crisis, data can help with identifying the location and number of people in need of aid, allocating resources efficiently and assessing the success and failures of a project. Even before the beginning of such a crisis, data can also be used to identify patterns and indicators associated with different types of threats (such as conflicts, natural disasters or epidemics), presenting huge opportunities for better-informed efforts to prevent violence and conflict.²² Data can also be used as (corroborating) evidence by human rights advocates to ensure accountability in case of human rights violations or other international crimes. For example, the Violations Documentation Center (VDC) collects data on the imprisonment, torture, disappearances and deaths of civilians, rebels, and regime forces in Syria to raise awareness in the international community and preserve evidence for potential future criminal investigations.²³

The emergence of new technologies provides increasing opportunities to collect invaluable data. In the span of a decade, there has been a significant proliferation of smartphones, as well as the rise and spread of drone technologies,²⁴ and the collection of biometrics (such as fingerprints and iris scans). These technologies were once reserved solely for governments and militaries, but have now become more affordable and, as a result, more accessible to the public.²⁵ For example, portable GPS devices, drones, infrared cameras, telephoto

²¹ Thomas Baar, Aikaterini Deligianni and Christoph Johann Stettina, ‘Data-Driven Innovation for NGO’s: How to Define and Mobilise the Data Revolution for Sustainable Development?’ (Data Policy Conference, Cambridge, September 2016) <www.researchgate.net/publication/311002010> accessed 16 June 2018 1.

²² Mary K Pratt, ‘Big Data’s Big Role in Humanitarian Aid’ (*Computerworld*, 6 February 2016) <www.computerworld.com/article/3027117/big-data/big-datas-big-role-in-humanitarian-aid.html> accessed 16 June 2018.

²³ The Engine Room, Benetech and Amnesty International, ‘Datnav: How to navigate digital data for human rights research’ (2016) 12 <www.theengineroom.org/wp-content/uploads/2016/09/datnav.pdf> accessed 16 June 2018.

²⁴ Lindsay Freeman, ‘Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials’ (2018) 41 *Fordham International Law Journal* 283, 288.

²⁵ *ibid.*

lenses, and satellite phones are all items ordinary citizens can now buy online.²⁶ Consequently, individuals and organizations have an unprecedented ability to access, collect, store and share data, especially in areas difficult to reach for reasons such as security concerns, infrastructure, and weather.²⁷

While data undoubtedly offers numerous opportunities to do good, they can also carry the potential to cause harm. Data tend to be sensitive, especially data relating to health, race, sexual orientation or ethnicity, religious/political/armed group affiliation, or genetic and biometric data. When disclosed, these data can be used to identify, locate and repress or discriminate the individuals concerned by the data processing, i.e. data subjects. In the most severe cases, data subjects can be exposed to physical harm, imprisonment or death. This is especially true of data collected about vulnerable data subjects, such as discriminated minorities or people living in armed conflicts. Even when not sensitive, or not collected in hostile environments, data can adversely affect data subjects, for example because data misuse results in identity theft, financial loss, or because the content of the data is *somewhat* sensitive.

These risks are further exacerbated by the increasing amount of data that new technologies allow to be collected. In addition, new threats linked with these technologies, such as cyber-warfare, digital crime and government surveillance, are becoming more widespread and frequent, particularly in unstable environments.²⁸ As more data systems and devices have become available, organizations, governments and private companies have been subjected to multiple cyber-crimes and targeted attacks and actions by groups with criminal or political motivations.²⁹ This was illustrated in 2018 by the scandal caused by Cambridge Analytica, a political consultancy firm that sold personal data from unaware Facebook users to companies and politicians.³⁰ The data obtained were used to profile voters and try to influence them with personalised political advertisements.

Processing data in the age of rapid technological advancement thus presents both many opportunities and risks at the same time. Fully harnessing the opportunities data offers to humanitarian, human rights and development organizations requires them to adopt a responsible approach to data, one that mitigates the

²⁶ Ben Wang and others, 'Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities' (2013) 2 *Stability: International Journal of Security and Development* 1, 2-3; Lindsay Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2018) 41 *Fordham International Law Journal* 283, 288.

²⁷ *ibid*; Council of the OECD, 'Revised Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (11 July 2013) (OECD); Patrick Meier, 'Big (Crisis) Data: Humanitarian Fact-Finding with Advanced Computing' in Philip Alston and Sarah Knuckey (eds), *The Transformation of Human Rights Fact-Finding* (Oxford University Press 2016) 495.

²⁸ OCHA Humanitarianism in the Age of Cyber (n 13) 5.

²⁹ The Engine Room, Benetech and Amnesty International (n 23) 12; OCHA Humanitarianism in the Age of Cyber (n 13) 2, 5-7, 12.

³⁰ 'Cambridge Analytica: Facebook data-harvest firm to shut' *BBC* (2 May 2018) <www.bbc.com/news/business-43983958> accessed 16 June 2018.

risks of harm inherent in data processing. Responsibly processing data is key, not only to protect data subjects (the very individuals that these organizations seek to assist through their data processing), but also to preserve the trust of these individuals in the organizations processing their data (an essential prerequisite for the success of the activities of the organizations in question). Failure to process data responsibly may also expose organizations to significant costs due to a discontinuation of the support of their donors, or as a result of legal liability when such failures amount to a violation of the data protection legislation a particular organization is subject to. A responsible approach to data therefore aids in mitigating the risks and harms to individuals that come with data processing, while at the same time improves the results of data processing activities and aids in the fulfilment of the underlying goals of the organizations concerned.

However, implementing a responsible approach to data is complicated for a number of reasons. Firstly, there is occasionally a lack of knowledge, on the part of those collecting and processing data, as to what a responsible approach to data could be, i.e. they might not be aware of what such an approach could entail, or how to establish their own responsible approach. A responsible approach to data has been defined for the purposes of this report as: “the duty to ensure individual consent, privacy, security and ownership around the data processes of collection, analysis, storage, presentation and reuse of data, while respecting the values of transparency and openness.”³¹ Such a responsible approach to data will be outlined by the present report as a whole. Secondly, where those collecting and processing data *are* aware of responsible approaches to data, there is also sometimes a lack of knowledge as to how to actually implement such an approach in practice.

This is often due to the fragmentation of the applicable data protection regulatory frameworks coexisting at national, regional and international level (discussed in chapter 2), which cause uncertainty, especially where data is collected, processed, and stored in different jurisdictions. In addition, the language of these regulatory frameworks is often very complex and can be difficult to understand. Conversely, certain frameworks can be very vague and provide little in the way of concrete guidance. Finally, the novelty of the data revolution, and of the technologies that have been developed as a result, also poses a problem, since there is a lack of awareness as to the risks to individuals posed by such technologies.

1.1. Aim of the Report

Bearing in mind these difficulties, the report aims to provide guidance for organizations working with data and seeking to process this data in a responsible manner, or to help them to improve their pre-existing policies. The report seeks to achieve this aim in three ways.

³¹ Responsible Data Forum (n 19) 16.

Firstly, the report outlines the core components (categorised in this report as either ‘entitlements’ or ‘principles’) of a responsible approach to data, as developed in existing instruments, be it regulatory frameworks, or guidelines developed by humanitarian, human rights and development organizations. The report therefore aims to give a comprehensive overview of the state of the art by mapping out the most developed components contained in instruments created by a diverse range of actors, each with their own individual experiences and strengths, culminating in a comprehensive guide to a responsible approach to data. Secondly, the report explains the scope and content of each of these core components, by breaking them down to be accessible and understandable, including for those not familiar with data processing and the potential risks arising therein. Finally, the report provides guidance on how to implement the components in practice, thereby making them workable for data practitioners. To that end, the report provides practical considerations, and highlights measures and tools developed by organizations, to effectively implement a responsible approach to data.

1.2. Research Approach

This section describes and explains the approach taken to conduct this research. This section first explains why the report studies regional and international data protection frameworks (‘regulatory frameworks’), as well as guidelines developed by humanitarian, human rights and development organizations in practice. This section then explains how the regulatory frameworks and the guidelines of organizations were selected. Finally, this section details how the comparative analysis, upon which the report was based, was conducted.

1.2.1. Reliance on Frameworks and Guidelines

This report studies two types of instrument developed to process data responsibly. In the first place, regulatory frameworks (at both the regional and international levels), developed by organizations such as the African Union (AU), the Council of Europe (CoE), or the Asia-Pacific Economic Cooperation (APEC), are considered. In addition, guidelines developed by organizations working in the humanitarian, human rights and development sectors, such as the International Committee of the Red Cross (ICRC), the International Organization for Migration (IOM), or Médecins Sans Frontières (MSF), are also considered. This choice stems from the complementary contributions of these two kinds of sources. While the regulatory frameworks generally provide an overview of the sorts of considerations to be borne in mind to process data responsibly, the guidelines add practical guidance, drawing on the first-hand experiences of the organizations that developed them.

By developing these regulatory frameworks, organizations such as the CoE were among the first to provide guidance as to how to responsibly process personal data.³² As such, these organizations have greatly influenced the current state of the art of responsible data processing. These regulatory frameworks were developed with a view to assisting national legislators in drafting legislation concerning personal data protection,³³ and many humanitarian, human rights and development organizations have drawn upon these frameworks to develop their own guidelines.

While the components of a responsible approach to data identified in the regulatory frameworks constitute an important source of inspiration and establish a solid structure for responsible data processing, some frameworks lack in detail (to allow a wide margin of flexibility for national legislators). In addition, when a framework is very detailed, (such as that of the European Union (EU) General Data Protection Regulation (GDPR), which came into force on 25 May 2018), the abundance of information can be too technical and difficult to digest, which poses challenges for non-lawyers or those who lack expertise in data processing. Another shortcoming of the regulatory frameworks is that they have struggled to keep pace with the technological developments. They rarely offer guidance into how to implement their identified components when using new technologies in processing data.

Consequently, sole reliance on these regulatory frameworks would not suffice to offer the practical guidance that this reports aims to provide. In this regard, it is important to highlight the role of a number of humanitarian, human rights and development organizations, which have taken it upon themselves to develop workable approaches to make their data processing activities more responsible. These guidelines are the result of the practical experience, successes and failures of these organizations, and provide operational (i.e. practical) value to the components identified in the regulatory frameworks.

This report focuses on regulatory frameworks which specifically deal with data protection. As a result, regional and international *human rights* frameworks are intentionally excluded from this report. This is due to the fact that, although some of the rights contained in human rights instruments may, in a way, be related to data protection (such as the right to privacy), they do not directly address this issue. Even in the limited cases where specific human rights systems explicitly recognise the existence of a right to data protection, the components of this right are not addressed in great depth. Furthermore, the purpose of the instruments in question as a whole do not concern the protection of data, unlike the regulatory frameworks studied in this report (the entire purpose of which is to address data protection). Therefore, human rights instruments

³² For more information regarding the year of adoption of the other guidelines, see Boxes 3 and 4.

³³ The GDPR constitutes an exception, as it directly binding on individuals and corporations, Damian Chalmers, Gareth Davis and Giorgio Monti, *European Union Law* (Cambridge University Press 2014) 112.

do not serve the purposes of this report; the relevant frameworks instead being those which relate directly to data protection.

1.2.2. Rationale of the Selection of Frameworks and Guidelines

This report relies on existing regulatory frameworks relating to data protection, with a view to rendering it as geographically inclusive as possible. For a list of these organizations, see chapter 2, concerning the regulatory framework identified, on pages 16 and 17. This report also relies on a selection of guidelines developed humanitarian, human rights and development organizations, which were selected on the basis of:

- i) the magnitude of their data processing activity, i.e. organizations which, due to their mandate and activities, collect and process considerable amounts of data; and/or
- ii) the comprehensiveness of their data processing guidelines, i.e. organizations which have developed guidelines offering high standards of data protection.

Accordingly, the organizations selected for the purposes of this report are:³⁴

- International Committee of the Red Cross (ICRC)³⁵
- International Organization for Migration (IOM)³⁶
- Médecins Sans Frontières (MSF)³⁷
- Office of the United Nations High Commissioner for Human Rights (OHCHR)³⁸
- Oxfam³⁹
- United Nations Development Group (UNDG)⁴⁰
- United Nations Global Pulse (UN Global Pulse)⁴¹

³⁴ See Table 2 on page 21.

³⁵ ICRC, 'ICRC Rules on Personal Data Protection' (ICRC 2016) <https://shop.icrc.org/icrc-rules-on-personal-data-protection.html?store=default&from_store=fr> accessed 21 June 2018 (ICRC Rules); ICRC Handbook (n 4).

³⁶ IOM (n 1).

³⁷ MSF, 'MSF Data Sharing Policy' (MSF 2013) <<http://fieldresearch.msf.org/msf/bitstream/10144/306501/1/MSF+data+sharing+policy+final+061213.pdf>> accessed 21 June 2018 (MSF).

³⁸ OHCHR, 'A Human Rights-based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development' (OHCHR 2015) <www.ohchr.org/Documents/Issues/HRIIndicators/GuidanceNoteonApproachtoData.pdf> accessed 9 June 2018 (OHCHR).

³⁹ Oxfam, 'Responsible Program Data Policy' (Oxfam 2015) <www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-responsible-program-data-policy-feb-2015-en.pdf> accessed 21 June 2018 (Oxfam).

⁴⁰ UNDG, 'Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda' (UNDG 2017) <https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf> accessed 21 June 2018 (UNDG).

⁴¹ UN Global Pulse, 'Big Data for Development and Humanitarian Action Towards Responsible Governance' (UN Global Pulse 2016) <http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_0.pdf> accessed 21 June 2018 (UN Global Pulse); UN Global Pulse, 'Privacy and Data protection Principles: Towards a Responsible Governance' (UN Global Pulse Big Data) <www.unglobalpulse.org/privacy-and-data-protection-principle> accessed 22 June 2018 (Un Global Pulse Principles).

- United Nations High Commissioner for Refugees (UNHCR)⁴²
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA)⁴³
- United States Agency for International Development (USAID)⁴⁴
- World Food Programme (WFP)⁴⁵

1.2.3. Comparative Analysis

This research was carried out by conducting a comparative analysis of the above-mentioned sources, with a view to identifying the different core components of a responsible approach to data, and providing the definition, content, and practical considerations and measures enabling the effective implementation, thereof. These components have been classified as either ‘entitlements of data subjects’ (discussed in chapter 3) or ‘data processing principles’ (discussed in chapter 4).

The present report discusses all entitlements and principles developed in the above-mentioned sources. The exceptions to this are the ‘right not to be put at risk’, referred to in Oxfam’s guidelines, and the ‘Preventing Harm Principle’ of the APEC Privacy Framework. However, in the other frameworks and guidelines studied, avoiding harm to data subjects resulting from data processing (known as the concept of ‘Do No Harm’), was instead conceptualised as one of the objectives of the frameworks and guidelines as a whole, rather than as an entitlement or principle in itself.⁴⁶ This approach was also followed for the purposes of the present report.

Sometimes the name given to a particular concept differed depending on the framework or guideline studied. For instance, the substance of the principles referred to in different frameworks or guidelines as either ‘data quality’ or ‘data accuracy’ is, in fact, the same. In this case, the most commonly used denomination was selected. Similarly, when the definition of a principle was divergent from source to source, the definition of the principle for the purposes of this report was selected on the basis on its clarity and the regularity of its use.

⁴² UNHCR, ‘Policy on the Protection of Personal Data of Persons of Concern to UNHCR’ (UNHCR 2015) <www.refworld.org/docid/55643c1d4.html> accessed 9 June 2018 (UNHCR).

⁴³ OCHA Humanitarianism in the Age of Cyber (n 13); Ziad Al Achkar and others, ‘Building Data Responsibility into Humanitarian Action’ (Lilian Barajas and Matthew Easton eds, OCHA Policy and Studies Series, OCHA 2016) <www.unocha.org/sites/unocha/files/Building%20data%20responsibility%20into%20humanitarian%20action.pdf> accessed 22 June 2018 (OCHA Building Data Responsibility).

⁴⁴ USAID, ‘ADS Chapter 508: Privacy Program’ (USAID 2014) <www.usaid.gov/sites/default/files/documents/1868/508.pdf> accessed 21 June 2018 (USAID).

⁴⁵ WFP (n 2).

⁴⁶ See e.g. WFP (n 2) 7; ICRC Handbook (n 4) 14; Organization of American States (Committee on Juridical and Political Affairs of the Permanent Council of the Organization of American States) ‘Preliminary Principles and Recommendations on Data Protection’ (17 October 2011) CP/CAJP-2921/10 (OAS Preliminary Principles) 3.

Some guidelines were more detailed than others with regard to the content of their entitlements and principles, or to the measures by which to implement them. Where this additional information offered interesting insights or practical solutions, it was relied upon in this report, in spite of the fact that it was not referred to in all frameworks and guidelines studied.

1.3. Limitations of the Report

This section highlights the limitations of this report, namely the focus on personal data and the exclusion of national legislation as one of the sources studied.

A first limitation of this report lies in its focus on the processing of personal data, i.e. “any information relating to an identified or identifiable natural person”,⁴⁷ which includes ‘personally identifiable information’ (PII). Some concerns have been raised about the harm that some categories of non-personal data can cause. This is the case, in particular, with regard to ‘demographically’ or ‘community identifiable information’ (DII or CII).⁴⁸ While these concerns are well-founded, the focus on personal data in this report stems from the fact that the material scope of most of the guidelines and regional frameworks studied is limited to personal data.⁴⁹ Consequently, issues related to DII or CII will be touched upon in chapter 5, where remaining challenges to be tackled in the field of data protection are identified.

A second limitation of this report lies in the exclusion of the different data protection legislation existing at the national level. National legislation concerning data protection remains very fragmented and dissimilar, raising challenges when attempting to identify a common approach to responsible data (discussed in chapter 2). Nevertheless, it should be highlighted that some of domestic data protection legislation is very comprehensive and developed and, as such, could have provided additional insight and information for the purposes of this report. However, it was not possible, nor was it the purpose of this report, to conduct an exhaustive review of all existing data protection legislation.

⁴⁷ ICRC Handbook (n 4) 9.

⁴⁸ See e.g. Linnet Taylor, ‘Group Privacy and Data Ethics in the Developing World’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017); Nathaniel Raymond, ‘Beyond “Do No Harm” and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data’ in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017).

⁴⁹ ICRC Handbook (n 4) 23; ICRC Rules (n 35) 31; IOM (n 1); WFP (n 2) 11; UNHCR (n 42) Article 1.3; USAID (n 44) section 508.1, 508.1.3; Asia-Pacific Economic Cooperation (Secretariat) ‘Privacy Framework’ (2005) APEC#205-SO-01.2 (APEC) 5; 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 (2016) OJ 2016 L 119/1 (GDPR) Article 2(1); OAS Preliminary Principles (n 46) 4; OECD (n 27) 13; ECOWAS, Supplementary Act on Personal Data Protection within ECOWAS (adopted 16 February 2010, entered into force) A/SA.1/01/10 (ECOWAS); the guidelines of NGOs such as Oxfam and MSF do not clearly specify their material scope of application but make reference to personal data. Two exceptions have been found, in the guidelines of OCHA and UNDG. Both guidelines deal with the risks of harm to groups or communities created by data collection, OCHA Humanitarianism in the Age of Cyber (n 43) 2; UNDG (n 40) 3.

Therefore, this report does not aim to provide a manual that will guarantee conformity with all existing applicable legal frameworks, but rather provides guidance that may be of help for organizations in respecting and implementing the goals of those frameworks. Because many of the International Organizations (IOs) studied in this report enjoy privileges and immunities at the national level, national and regional legislation concerning data protection does not formally apply to them. Thus, it is possible that some of the guidelines of these IOs studied fall short of the requirements of the most detailed national data protection legislation, or some of the most comprehensive regulatory frameworks, such as the EU GDPR. Consequently, data controllers drawing upon the guidelines studied in the present report should ensure that they fully comply with the specific legislation to which they are subject, which, as will be discussed in chapter 2, depends on different considerations, such as where the organization is registered, where it operates, or the type of data that is processed.

1.4. Structure of the Report

In chapter 2, the report will outline and discuss the existing regulatory landscape concerning data protection. Immediately following, Tables 1 and 2 indicate the extent to which the entitlements and principles identified for the purposes of this report are included in the frameworks and the guidelines of the organizations identified above. Chapter 3 will focus on the identified entitlements of data subjects, providing a definition of each, followed by a description of how the entitlements can be implemented in practice. Chapter 4 will then consider the identified data protection principles, again providing a definition, a description of the substance of each principle, and how they can be implemented in practice. Finally, further challenges in this field will be considered, and a number of conclusions will be drawn.

2. THE EXISTING REGULATORY LANDSCAPE

This chapter describes the existing ‘regulatory’ landscape concerning data protection. As will be seen, data protection has been addressed at the national, regional and international level; however, not in equal measure. For the purposes of this report, the term ‘regulatory’ is intended to encompass both legally binding and non-legally binding (or policy) instruments. National legislation and certain regional and international frameworks (such as the EU GDPR or the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) establish legal requirements; while others are of a non-legally binding nature (such as the OECD Privacy Guidelines or the APEC Privacy Framework), and are aimed at recommending and offering some guidance to states about the minimum standards that a data protection policy should have.

The fragmentation of this existing landscape creates uncertainty regarding the rules applicable to data processing. On the one hand, at the national level, data protection legislation remains very dissimilar and there is a lack of coherence. On the other hand, at the regional and international levels it is possible to identify some commonalities within the existing instruments, in terms of the content of these instruments and the different entitlements and principles discussed therein.⁵⁰ Although these regional and international instruments could provide a basis for a unified approach to data protection, they are either lacking in detail, or are too technical, which poses challenges concerning their implementation in practice. There thus remains the need for a more comprehensive, accessible and practical approach to data protection.

This chapter is divided into three sections. The first section highlights the existing fragmentation and disparity at the national level. The second and third sections then provide an outlook of the current data protection instruments at the regional and international levels respectively. These regional and international instruments are categorised for the purposes of this report as 'regulatory frameworks'. Finally, this section concludes in highlighting the strengths and weakness offered by the regulatory frameworks and, in doing so, it serves as a justification for the approach adopted in this project, namely a comparative approach, combining the regulatory frameworks with the guidelines of other organizations which have practical experience processing data.

2.1. The National Level

At the national level, data protection frameworks are characterised by disparity. Despite the increasing growth of data protection legislation, nearly thirty percent of all states have no laws in place whatsoever.⁵¹ As exemplified by Figure 1, some states have adopted very strict and comprehensive data protection legislation, while others have very loose legislation or none in place at all. As a result, even where there is legislation in place, significant differences exist from state to state. For example, some laws only apply to sensitive data; others are restricted to either online or offline data processing; others still are restricted to specific sectors such as health; while some allow for notable derogations and exceptions in the application of the legislation.⁵²

⁵⁰ See Table 1 on page 20.

⁵¹ United Nations Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (United Nations 2016) 8 <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 21 June 2018.

⁵² *ibid.*

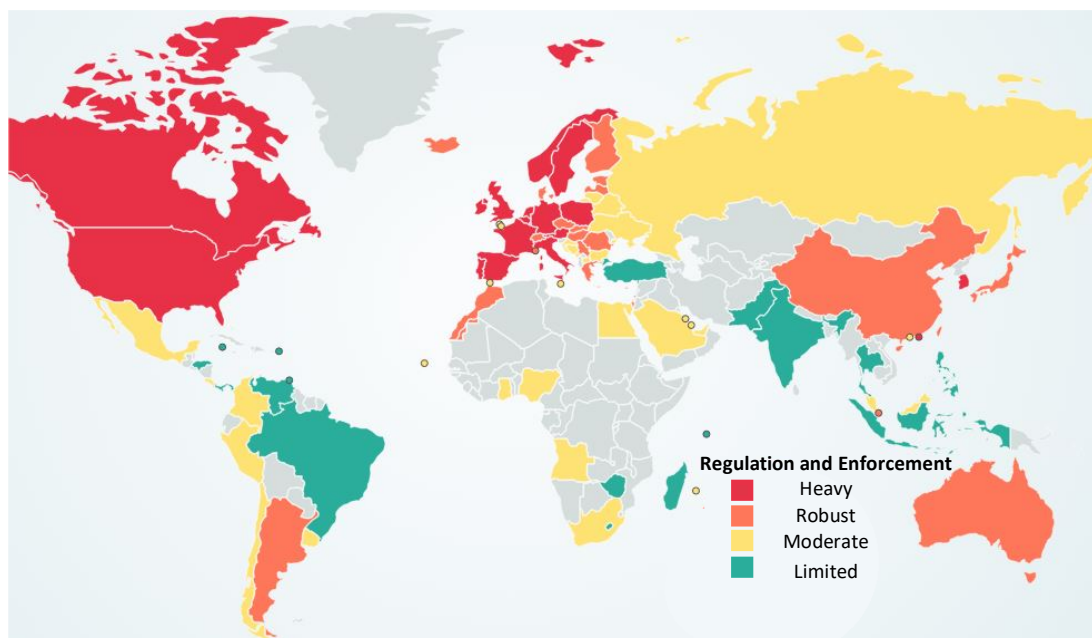


Figure 1: Data Protection Laws of the World⁵³

These disparities, and the lack of general coherence within national data protection legislation, create serious concerns, especially when dealing with data processing (including, *inter alia*, the collection, use and storage of data) which takes place in different jurisdictions. Different laws may apply depending on, for instance, where the data controllers are registered or where the data subjects reside. It is therefore highly recommended that organizations take the time to investigate the domestic laws applicable to them and their work. In order to establish which domestic regime applies, organizations should consider the most common grounds for jurisdiction regarding data processing, i.e. the determination of what legislation applies to certain data processing activities, and when (Box 1).⁵⁴

Box 1: Grounds for Jurisdiction Regarding Data Processing

- | | |
|---|--|
| <ul style="list-style-type: none"> • Jurisdiction where the data controller is registered • Jurisdiction where the data controller operates | <ul style="list-style-type: none"> • Jurisdiction where the data subjects are • Jurisdiction where the data are stored |
|---|--|

In addition, the increasing reliance on cloud computing (the use of various services, such as servers, storage and software, over the internet) when dealing with data further complicates the assessment of which domestic jurisdiction is applicable. This complexity regarding jurisdictional issues and cloud computing can be exemplified by the case of *United States v Microsoft Corp.*⁵⁵ As part of the investigation into another case in 2013, Microsoft did not comply with a warrant issued by the US District Court requesting data stored on a server in Ireland. Microsoft claimed that the data fell within the jurisdiction of Ireland and was

⁵³ 'Data protection Laws of the world' (DLA Piper, 2018) <www.dlapiperdataprotection.com> accessed 17 June 2018.

⁵⁴ Responsible Data Forum (n 19) 46.

⁵⁵ *United States v Microsoft Corporation*, 584 US Supreme Court (2018).

consequently protected by Irish privacy legislation. However, the US District Court held Microsoft in contempt for non-compliance with the warrant.⁵⁶ Nevertheless, on appeal to the US Court of Appeals to the Second Circuit, this judgment was overturned and the warrant invalidated. The case was again appealed and was finally heard at the US Supreme Court in February 2018, but never came to a conclusion due to the enactment of a new piece of US legislation, the Clarifying Lawful Overseas Use of Data (CLOUD) Act. This legislation provides that US law enforcement orders may reach certain data located in other countries, and therefore rendered the case moot.⁵⁷

In addition to these jurisdictional issues, sometimes the applicable laws will vary depending on a range of other considerations, such as the type of data with which the organizations work (see Box 2).⁵⁸

Box 2: Other Considerations in the Application of Legislation

- Sensitivity of the data (e.g. health or financial records)
- Sources of the data (e.g. online or offline data collection)
- Sector of the organization (e.g. public sector, private sector, health sector or financial sector)

Therefore, the existing legal framework at the national level remains unclear and highly fragmented, with different, and sometimes even contradictory, data protection legislation attempting to regulate data processing. As a result, there is a lack of clarity, in turn creating uncertainty, regarding which laws should apply to data processing in the digital age. For these reasons, domestic instruments for data protection will not be considered for the purposes of this report.

2.2. The Regional Level

At the regional level, there have been some efforts to establish a common approach to data protection. These regional efforts help to counterbalance the existing fragmentation at the national level by attempting to harmonise the data protection legislation of specific groups of states. The regional frameworks considered for the purposes of this study are the:

- Asia Pacific Economic Cooperation (APEC) Privacy Framework;⁵⁹

⁵⁶ Ellen Nakashima, 'Supreme Court to hear Microsoft case: A question of law and borders' *The Washington Post* (Washington, February 25, 2018) <www.washingtonpost.com/world/national-security/supreme-court-case-centers-on-law-enforcement-access-to-data-held-overseas/2018/02/25/756f7ce8-1a2f-11e8-b2d9-08e748f892c0_story.html?utm_term=.8ee2b53555eb> accessed 17 June 2018; Louise Matsakis, 'Microsoft's Supreme Court Case has Big Implications for Data' (*WIRED*, February 27, 2018) <<https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/>> accessed 17 June 2018; Emily Skahill, 'Head in THE Cloud(s): What the U.S. v. Microsoft Case reveals about the Governmental Ramifications of Cloud Computing' *Brown Political Review* (April 7, 2018) <<http://www.brownpoliticalreview.org/2018/04/head-clouds-u-s-v-microsoft-case-reveals-governmental-ramifications-cloud-computing/>>.

⁵⁷ Brian P Goldman, Robert Loeb and Emily S Tabatabai, 'The CLOUD Act explained' *Orrick* (April 6, 2018) <<https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained>>.

⁵⁸ United Nations Conference on Trade and Development (n53) 9.

⁵⁹ APEC (n 49).

- African Union (AU) Convention on Cyber Security and Personal Data Protection;⁶⁰
- Commonwealth Model Bill on the Protection of Personal Information;⁶¹
- Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection;⁶²
- European Union (EU) General Data Protection Regulation (GDPR);⁶³ and the
- Organization of American States (OAS) Principles and Recommendations on Data Protection.⁶⁴

These regional efforts vary in terms of scope and application. Box 3 compiles the relevant information for each regional framework relied on for the purposes of this report.

Box 3: Regional Frameworks on Data Protection			
Regional Frameworks	Year	Membership	Legal force
APEC: Privacy Framework	2005	APEC members	Non-binding
AU: Convention on Cyber Security and Personal Data Protection	2014, not yet in force	AU members (2 ratifications to date)	Binding
Commonwealth: Model Bill on the Protection of Personal Information	2005	Commonwealth members	Non-binding
ECOWAS: Supplementary Act on Personal Data Protection	2010	ECOWAS members	Binding
EU: GDPR	2016, in force 2018	EU members	Binding
OAS: Preliminary Principles and Recommendations on Data Protection	2011	OAS members	Non-binding

There are also important differences in terms of enforcement of these regional frameworks, with some being merely recommendatory or dependant on voluntary application, i.e. non-binding. Others have binding force and, as such, impose legal obligations on the states parties to them. Among these regional regulatory frameworks, the EU GDPR stands out, being one of the most recent instruments concerning data protection,

⁶⁰ African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) (AU Malabo Convention).

⁶¹ Commonwealth (Commonwealth Law Ministries and Secretariat) 'Model Bill on the Protection of Personal Information' (approved by the Commonwealth Law Ministries 17 October 2005, published by the Secretariat 2017) (Commonwealth Model Bill).

⁶² ECOWAS (n 49).

⁶³ GDPR (n 49).

⁶⁴ OAS Preliminary Principles (n 46).

and “setting out some of the highest standards of data protection in the world”.⁶⁵ The GDPR, unlike its predecessor the 1995 Data Protection Directive, has direct effect in all EU member states.⁶⁶ In addition, the GDPR has a wide scope of application as it covers processing activities carried out by any data controller or processor established in the EU (even when the processing does not take place within the EU), as well as the processing of the personal data of data subjects with EU citizenship (even when the processing is carried out by a controller or processor not established in the EU).⁶⁷

A final recent development was the publication of the Personal Data Protection Guidelines for Africa in May 2018, aimed at facilitating the implementation of the AU Convention on Cyber Security and Personal Data Protection.⁶⁸ These Guidelines offer recommendations and give more specific guidance regarding some of the principles set out in the Convention.

2.3. The International Level

Some of the regulatory frameworks developed are international, in that they are open to all states instead of being addressed to a specific group of states (as is the case with the regional frameworks). Under this category, two notable data protection frameworks are the:

- CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108);⁶⁹ and the
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.⁷⁰

The OECD Guidelines are not legally binding. Nevertheless, the principles contained in these Guidelines have influenced the content of data protection laws around the world.⁷¹ The CoE Convention 108 is the only binding international legal instrument concerning data protection. In addition to having been ratified by all 47 members of the CoE, the Convention has so far been ratified by 5 additional states. Furthermore, a Protocol amending the Convention, with a view to modernising it and bring it up to date with the GDPR, was introduced in May 2018. This Protocol would make amendments such as: explicitly making reference to the

⁶⁵ European Union (European Commission) ‘Communication from the Commission to the European Parliament and the Council on Stronger Protection, New Opportunities: Commission guidance on the direct application of the application of the General Data Protection Regulation as of 25 May 2018 (2018) 43.

⁶⁶ “A ‘regulation’ is a binding legislative act. It must be applied in its entirety across the EU”. “A ‘directive’ is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how.” One of the strengths of the GDPR is that it is a regulation, while its predecessor was a directive. ‘Regulations, Directives, and other Acts’ (*European Union*, 22 June 2018) <https://europa.eu/european-union/eu-law/legal-acts_en> accessed 22 June 2018.

⁶⁷ GDPR (n 49) Article 3.

⁶⁸ African Union (Commission of the African Union and Internet Society) ‘Personal Data Protection Guidelines for Africa’ (9 May 2018) (AU Guidelines).

⁶⁹ Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (opened for signature 28 January 1981, entered into force 1 October 1985) ETS 108 (CoE Convention 108).

⁷⁰ OECD (n 27).

⁷¹ United Nations Conference on Trade and Development (n 58) 26.

need for consent as a legitimate basis for data processing; expanding the list of sensitive data; and introducing an obligation to ensure the transparency of data processing.

Box 4: International Frameworks on Data Protection			
International Frameworks	Year	Membership	Legal force
CoE: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)	1981, in force 1985	Open to any country (52 ratifications to date)	Binding
<i>Protocol Amending Convention 108</i>	<i>Opened for signature 25 June 2018</i>	<i>Open to any country (which has ratified the Convention)</i>	<i>Binding</i>
OECD: Privacy Framework	1980, revised in 2013	Open to any country	Non-binding

Recognising the importance of international frameworks, the 30th International Conference of Data Protection and Privacy Commissioners, adopted a resolution stating that the next stage of recognition of the right to privacy and data protection requires:

The adoption of a universal legally binding instrument establishing, drawing on and complementing the common data protection and privacy principles laid down in several existing instruments and strengthening the international cooperation between data protection authorities.⁷²

The same conference adopted the International Standards on the Protection of Personal Data and Privacy, also known as ‘The Madrid Resolution’, a year later. This document seeks to reflect the many data protection approaches worldwide and, in doing so, stresses the universal nature of the principles and guarantees underlying data protection.⁷³

2.4. Concluding Remarks

Following an overview of the existing regulatory landscape, it can be deduced that despite their differences in scope and legal applicability, there is a remarkable degree of harmonisation and coherence among the entitlements and principles identified in the regulatory frameworks at the regional and international

⁷² ‘Resolution on the urgent need for protection privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection’ (International Conference on Data Protection and Privacy Commissioners, Strasbourg, 17 October 2008) <<https://icdppc.org/wp-content/uploads/2015/02/Resoltuion-on-the-urgent-need-for-protecting-privacy-in-a-borderless-world.pdf>> accessed 22 June 2018.

⁷³ ‘International Standards on the Protection of Personal Data and Privacy’ (International Conference of Data Protection and Privacy Commissioners, 5 November 2009) <https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf> accessed 22 June 2018.

levels,⁷⁴ (as can be observed from Table 1 on page 20). Nevertheless, it must be highlighted that, even though these regulatory frameworks identify similar entitlements and principles, there is still a need for further guidance.

This is mainly for two reasons. Some frameworks are lacking in detail and substance, to allow states a wide margin of flexibility when implementing the frameworks at the national level by way of domestic legislation. Other frameworks are very detailed. However, when this is the case, such as with the EU GDPR, the bulk of information can be too technical and difficult to digest, creating implementation challenges for non-lawyers or those lacking expertise in data protection. Consequently, either due to a lack of detail or a lack of clarity, there is a need to further develop the substance of each entitlement and principle identified in these frameworks, as well as the methods by which they can be implemented in practice. Moreover, these frameworks do not make direct reference to the risks posed by processing data in the digital age, nor do they provide practical considerations for processing data responsibly when using new technologies. Therefore, while these regulatory frameworks establish a solid structure, there remains a need to give each entitlement and principle identified within true operational value, in particular by way of additional practical guidance.

In this context, it is important to highlight the role of organizations in the humanitarian, human rights and development sectors that have taken it upon themselves to develop workable policies to guide their data processing activities. These guidelines are the product of the organizations' practical experience, successes and failures, and can provide a source of inspiration for both legislators and other organizations seeking to develop their own responsible approaches to data collection. Table 2 (on page 21) illustrates that the guidelines studied for the purposes of this report enjoy a high degree of coherence, identifying and elaborating on many similar entitlements and principles. In creating these guidelines, a number of the organizations have drawn inspiration from the current regulatory landscape described above. For instance, according to the ICRC, the guidelines contained in their Handbook are based, *inter alia*, on the OECD Privacy Framework, the CoE Convention 108 and the EU GDPR. However, building on these existing frameworks, these guidelines provide additional practical guidance, mechanisms and examples regarding responsible approaches to data processing, and often explicitly make considerations regarding new technologies. The regulatory frameworks and the guidelines of humanitarian, human rights and development organizations therefore complement each other and, when combined, can provide the basis for a responsible approach to data in the digital age. For this reason, this report draws on both of these types of instruments and considers their approaches together.

⁷⁴ United Nations Conference on Trade and Development (n 58) 2.

Table 1: Entitlements and Principles Identified in Regulatory Frameworks

Legend	
Clearly Identified	
Briefly Mentioned	
Not Found	

		Regional Frameworks						International Frameworks	
		APEC	AU	Commonwealth	ECOWAS	EU	OAS	CoE	OECD
Entitlements of Data Subjects	Privacy								
	Information								
	Access								
	Correction								
	Erasure								
	Objection								
	Participation								
Data Protection Principles	Legitimate Processing								
	Informed Consent								
	Purpose Limitation								
	Data Minimisation								
	Storage Limitation								
	Data Quality								
	Transparency and Openness								
	Data Security								
	Accountability								

Table 2: Entitlements and Principles Identified in Guidelines

Legend	
Clearly Identified	
Briefly Mentioned	
Not Found	

		ICRC	IOM	MSF	OCHA	OHCHR	Oxfam	UNDG	UN Global Pulse	UNHCR	USAID	WFP
Entitlements of Data Subjects	Privacy											
	Information											
	Access											
	Correction											
	Erasure											
	Objection											
	Participation											
Data Protection Principles	Legitimate Processing											
	Informed Consent											
	Purpose Limitation											
	Data Minimisation											
	Storage Limitation											
	Data Quality											
	Transparency and Openness											
	Data Security											
	Accountability											

3. ENTITLEMENTS OF DATA SUBJECTS

3.1. Introduction

For the purposes of this report, a number of entitlements of data subjects have been identified, namely privacy, information, access, correction, erasure, objection, and participation. Respect for these entitlements, addressed to individual data subjects (who, in turn, can exercise them), should be at the core of any responsible data protection policy.

Most of the regulatory frameworks and guidelines studied in this report refer to the universally recognised human right to privacy in their introductory matter. The Human Rights Committee has interpreted the right to privacy under International Covenant on Civil and Political Rights (ICCPR)⁷⁵ to include:

The right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.⁷⁶

The human right to privacy under the ICCPR has therefore been interpreted to encompass a right to information, access, correction and erasure; however, there is no mention of a right to objection.⁷⁷ Nevertheless, in addition to the other rights mentioned, the right to objection has been recognised in some of the international and regional instruments (regulatory frameworks) studied in this report, both legally binding⁷⁸ and non-binding,⁷⁹ as can be seen from Table 1 (on page 20). Furthermore, as can be seen from Table 2 (on page 21), a number of the guidelines of humanitarian, human rights and development organizations studied also explicitly refer to these ‘rights of data subjects’, including information, access, correction, erasure and objection.⁸⁰

While participation in public affairs is also recognised as a human right under the ICCPR,⁸¹ participation in the sense in which this report refers to the concept (i.e. participation in data processing exercises), is not covered within the scope of this human right.

⁷⁵ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) Article 17.

⁷⁶ Human Rights Committee, General Comment 16, UN Doc HRI/GEN/1/Rev.9 para 10.

⁷⁷ Which has been identified as an entitlement of data subjects for the purposes of this report.

⁷⁸ CoE Convention 108 (n 69) Article 9(1); GDPR (n 49) Article 21; AU Malabo Convention (n 60) Article 18; ECOWAS (n 49) Article 40.

⁷⁹ AU Guidelines (n 68) 16; OAS Preliminary Principles (n 46) Principle 11.

⁸⁰ See e.g. ICRC Handbook (n 4); UNHCR (n 42); OCHA Humanitarianism in the Age of Cyber (n 13).

⁸¹ ICCPR, Article 25(a).

Therefore, for the purposes of this report, the term ‘entitlements’ has been selected as a preferable alternative to the term ‘rights’. This choice is based on a number of factors. Firstly, the regulatory frameworks referred to in this report are not all *legally binding* instruments. Therefore, when the term ‘right’ is adopted in a *non-legally binding* instrument, this may be in reference to something that is accepted as a legal right. However, this is not always the case. Moreover, as highlighted in chapter 2, the current regulatory framework is characterised by disparity (without a universally ratified overarching data protection framework), and rights recognised in one region or, indeed, at the national level in one state, may not be recognised in another. For example, objection is not recognised as a right in all of the regulatory frameworks studied,⁸² and participation (in the context of this report) is not recognised as a right at all. As a result, the report cannot justifiably refer to all of these concepts within one category of ‘rights’.

Secondly, human rights are *prima facie* only binding on states (meaning that the obligation to respect human rights lies with the government) and, therefore, the language of ‘rights’ is not necessarily the most appropriate for the primary audience of this study, namely organizations collecting and processing data. In addition, even where legislation conferring legal rights on data subjects has been implemented at the national level (meaning that actors other than the state may be compelled to respect certain rights of data subjects), some organizations, namely international organizations enjoying privileges and immunities, are not subject to national legislation.⁸³ Therefore, an individual data subject may still not be able to bring a claim against certain organizations before a court or data protection authority.⁸⁴

Accordingly, for the avoidance of confusion, and to facilitate the reading and implementation of this report, the concepts outlined above will be referred to as ‘entitlements’, despite the fact that some may amount to legal rights in certain jurisdictions.

In this chapter, the entitlements to privacy, information, access, correction, erasure, objection, and participation will first each be defined, followed by an explanation of the substance⁸⁵ of the entitlement and guidance for its implementation in practice.

⁸² APEC (n 49), Commonwealth Model Bill (n 61), and OECD (n 27) do not recognise objection.

⁸³ This could also apply to some regional instruments with direct effect, such as the EU GDPR (n 49).

⁸⁴ ICRC Handbook (n 4) 38.

⁸⁵ Within chapter 3, the entitlements of data subjects will not be divided into separate ‘substance’ and ‘in practice’ subsections, as is the case in chapter 4. These subsections are amalgamated in this chapter due to the nature of the entitlements and the fact that there is less information distinguishing between the substance of the entitlement and its implementation in practice in the documents studied (partly due to the fact that, as will be seen, the data protection principles largely provide mechanisms by which to implement the entitlements).

3.2. Privacy

3.2.1. Definition

Data subjects should have control over who can access and manage their personal data. Unless consented thereto, data disclosed to data controller should be protected and kept private.⁸⁶

3.2.2. The Entitlement in Practice

Data subjects are entitled to privacy in the treatment of their data and it is the responsibility of data controllers “to protect the identity of those providing data, unless otherwise outlined and agreed to in the informed consent.”⁸⁷

3.2.2.1. Data Collection and Use

The process of data collection should be conducted in an environment where the privacy of the data subject is upheld.⁸⁸ Accordingly, entities dealing with data should not access, analyse, or use the content of private communications without the knowledge or proper consent of the individual.⁸⁹ To ensure the privacy of the data subjects concerned, data controllers should have in place collection and management systems that are equipped to protect the privacy of individuals at every stage in the data gathering process.⁹⁰ Moreover, entities processing data should not knowingly or purposefully access, analyse, or otherwise use personal data, which was shared by an individual with a reasonable expectation of privacy without the knowledge or consent of the individual.⁹¹

UNHCR staff have used a mobile application ('app') at the Za'atari refugee camp in Jordan to scan the barcodes found on refugees' identity documents and verify whether they are eligible for a range of services, such as food, clothing, or cash aid. The app does not show the individual's name and picture, ensuring that the refugee's privacy is protected.

92

⁸⁶ Legal instruments and guidelines containing the right to privacy: Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) (UDHR) Articles 7, 12, 13; European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1990) ETS 5, 213 UNTS 221 Article 8; American Convention on Human Rights (adopted 22 November 1969, entry into force 18 July 1978) OAS Treaty Series No 36 Article 11; ICCPR Articles 12, 17, 26; United Nations Human Rights Committee UNHRC 'General Comment 16' in 'Article 17, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (adopted 8 April 1988) HRI/GEN/1/Rev.9 (Vol. I); Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 Articles 2, 12, 16; International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3 Articles 1, 8, 14; OHCHR (n 38) 14; Commonwealth Model Bill (n 61) Article 3; OECD (n 27) 3; APEC (n 49) 2-4; CoE Convention 108 (n 69) Article 1; AU Malabo Convention (n 60) Article 13, 14 and 25; AU Guidelines (n 68) 2 and 4-5; ECOWAS (n 49) Article 2 and 36; OAS Preliminary Principles (n 46) 2; IOM (n 1) 3, 9 and 13; MSF (n 37) 4; ICRC Handbook (n 4) 7 and 15; Oxfam (n 39) 3-4; UNHCR (n 42) 17.

⁸⁷ Oxfam (n 39) 3-4; UNHCR (n 42) 17.

⁸⁸ Oxfam (n 39) 3-4.

⁸⁹ UN Global Pulse Principles (n 41); OHCHR (n 38) 15.

⁹⁰ *ibid*; IOM (n 1) 11, 13.

⁹¹ *ibid*.

⁹² Kenechi Okelele, 'Refugees and Identity: Considerations for Mobile-Enabled Registration and Aid Delivery' (GSMA 2017) 12 <www.gsmaintelligence.com/research/2017/09/refugees-and-identity-considerations-for-mobile-enabled-registration-and-aid-

Organizations should not knowingly and purposefully attempt to re-identify de-identified data, and should make all reasonable efforts to prevent any unlawful and unjustified re-identification.⁹³ Data controllers thus need to ensure that personally identifiable information (PII) is separated from other data collected and kept in a manner that allows for it to be fully protected.⁹⁴ PII is any information or data related to an individual who can be identified either from that data; from that data and other information; or by means reasonably likely to be used related to that data.⁹⁵

Box 5: Examples of Personally Identifiable Information (PII)

- | | |
|--|--|
| <ul style="list-style-type: none"> • Name • Sex • Gender • Marital status • Data and place of birth • Occupation | <ul style="list-style-type: none"> • Fingerprint⁹⁶ • Iris scan • Expressions of opinion • Results from a needs assessment⁹⁷ • Religion • Ethnicity |
|--|--|

The UNHCR is collecting biometric data (iris scans and fingerprints) from Syrian refugees living in Jordan. The UNHCR have shared this data with the Cairo-Amman Bank, enabling refugee account-holders to withdraw cash from special ATMs simply by having their iris scanned. In this regard, the UNHCR have assured the refugees that the data will remain between them and the bank.

98

Data subjects should be reassured about an organization's commitment to privacy, since this will enhance the reliability and correctness of the gathered information.⁹⁹ This commitment to confidentiality, with the expectation that the personal data would not be disclosed in ways that are contrary to the wishes of the data subject, should also be included in contractual clauses with personnel and third parties.¹⁰⁰ In addition, all representatives of authorised third parties should be bound by the condition of confidentiality.¹⁰¹

[delivery/644/](#)> accessed 21 June 2018; Ben Parker, 'Aid's cash revolution: a numbers game' *IRIN News* (Bekka Valley, 2 November 2016) <www.irinnews.org/feature/2016/11/02/aid%E2%80%99s-cash-revolution-numbers-game> accessed 21 June 2018; Mats Granryd, 'Five ways mobile technology can help in humanitarian emergencies' (*World Economic Forum*, 22 August 2017) <www.weforum.org/agenda/2017/08/mobile-technology-humanitarian-crisis/> accessed 21 June 2018.

⁹³ UN Global Pulse Principles (n 41).

⁹⁴ OHCHR (n 38) 14.

⁹⁵ UNHCR (n 42) 11.

⁹⁶ Fingerprints and iris scans are examples of biometric data, which is a personal biological (anatomical or physiological) or behavioural characteristic which can be used to establish a person's identity by comparing it with stored reference data: UNHCR (n 42) 11.

⁹⁷ USAID (n 44) 6-7.

⁹⁸ Charlie Dunmore, 'Iris scan system provides cash lifeline to Syrian refugees in Jordan' (*UNHCR*, 23 March 2015) <www.unhcr.org/news/latest/2015/3/550fe6ab9/iris-scan-system-provides-cash-lifeline-syrian-refugees-jordan.html> accessed 21 June 2018; 'Syrian Aid in the Tech Age' *IRIN News* (Amman, 14 November 2013) <www.irinnews.org/report/99127/syrian-aid-tech-age> accessed 22 June 2018.

⁹⁹ IOM (n 1) 59.

¹⁰⁰ Oxfam (n 39) 3-4; IOM (n 1) 59-60.

¹⁰¹ IOM (n 1) 59.

3.2.2.2. Data Sharing

Data disclosed to data controllers should be protected and kept private, and only shared with authorised third parties when the data subject has consented thereto.¹⁰² For instance, the IOM's guidelines state that information gathered from participants should not be discussed or shared, in any form, with unauthorised individuals or entities. Given the sensitivity of the data at hand, data controllers should take due care when authorising the disclosure of personal data, since breaches of confidentiality may result in a multitude of protection problems such as harm or threat to life, discriminatory treatment and detention.¹⁰³ In some situations, organizations processing data in developing countries have been faced with the challenge of ensuring that data subjects are not subject to negative personal repercussions on the basis of identifying details that are revealed when research findings are reported.¹⁰⁴

Consequently, information that identifies individuals or discloses an individual's personal characteristics should not be made public without an assessment of the potential impact and the data subject's consent.¹⁰⁵ Moreover, in a more stringent manner, the OHCHR has expressed that data should not be published or made publicly accessible in a manner that permits identification of individual data subjects, either directly or indirectly.¹⁰⁶ Editing out the names and other relevant information of individuals does not always prevent a re-identifying process. There are multiple tactics for re-identifying data, where presumably anonymous data sets are combined with powerful algorithms and other datasets to identify individuals and their activity, also called the 'mosaic effect'.¹⁰⁷ The mosaic effect occurs when disparate datasets or various apparently unrelated data points are combined to reveal sensitive information or the data subject's identity.¹⁰⁸ For example, if a dataset has two attributes, say A and B, for an individual, when A and B are combined with another dataset that shows B and C with a geographic location, individuals can be identified.¹⁰⁹ This phenomenon is especially problematic because it can be hard to estimate the chances that any given dataset can be re-identified, since it is not possible to anticipate all the datasets that might be produced and engaged with.¹¹⁰

¹⁰² Karin Clark and others, *Guidelines for the Ethical Use of Digital Data in Human Research* (The University of Melbourne and Carlton Connect Initiative 2015) 11; OHCHR (n 38) 14.

¹⁰³ IOM (n 1) 59.

¹⁰⁴ Lorraine Young and Hazel Barrett, 'Ethics and participation: Reflections on research with street children' (2001) 4 *Ethics, Place & Environment* 130, 134; UNICEF, 'Ethical Principles, Dilemmas and Risks in Collecting Data on Violence against Children: A review of Available Literature' (UNICEF 2012) 47 <https://data.unicef.org/wp-content/uploads/2015/12/EPDRCLitReview_193.pdf> accessed 22 June 2018.

¹⁰⁵ See the principle of informed consent in chapter 4; OHCHR (n 38) 14-15; UNICEF (2012) 47.

¹⁰⁶ OHCHR (n 38) 14; UNHCR (n 42) 15.

¹⁰⁷ Responsible Data Forum (n 19) 22.

¹⁰⁸ Dale Neef, *Digital Exhaust: What Everyone Should Know about Big Data, Digitization and Digitally Driven Innovation* (Pearson Education 2014) 224.

¹⁰⁹ Glenn Richardson (ed), *Social Media and Politics: A New Way to Participate in the Political Process* (ABC-CLIO 2016) 74.

¹¹⁰ Responsible Data Forum (n 19) 22.

The risk of re-identification was illustrated by the New York Taxi (2014) case study. Under a Freedom of Information Request, New York City released data on 192 million taxi trips and fares made in the previous year, containing data on details such as pick up and drop off points. This data held a lot of potential research benefits and could be of great use to city planners. However, it also contained PII, such as the name of the driver, taxi license and taxi plate number. The PII was supposed to be kept separate and protected by a method known as “hashing”. However, due to a poor understanding of this method, the taxi license numbers were limited to only three million possible combinations. It took only minutes, using a modern computer, to reverse the anonymising method and reveal the taxi license numbers. Moreover, since the NYC Taxi and Limousine Commission also provided data linking real names to taxi license numbers, researchers could find the name of the driver of nearly every single one of the 192 million journeys. From this, it was possible to determine how much the driver earned, where they lived and when they worked.

111

In cases such as human rights monitoring, however, it can also be necessary and useful to publish data that identifies individuals.¹¹² This may be the case when an individual has been the victim of a crime or human rights violation and the publication of information about the incident is necessary to ensure perpetrator accountability. Data controllers should always weigh the impacts on the individual and on those associated with them before publishing data of this nature.¹¹³ Moreover, this should only be done where strictly necessary, and where permission has been given by the individual concerned. In the case of persons who are deceased or who have been kidnapped, detained or disappeared, permission could come from their family or close associates.¹¹⁴

3.3. Information

3.3.1. Definition

Data subjects are entitled to be made aware of the fact that they are participating in the data processing. There exists a minimum amount of information about the collection and processing of personal data that should be disclosed to data subjects.¹¹⁵

¹¹¹ Responsible Data Forum (n 19) 93; NYC Taxi and Limousine Commission, 'NYC Taxi Trip Data 2013' (FOIA/FOIL) <<https://archive.org/details/nycTaxiTripData2013>> accessed 21 June 2018; Vijay Pandurangan, 'On Taxis and Rainbows: Lessons from NYC's improperly anonymized taxi logs' (*Tech Vijayp*, 21 June 2014) <<https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1>> accessed 21 June 2018.

¹¹² OHCHR (n 38) 15.

¹¹³ *ibid.*

¹¹⁴ *ibid.*

¹¹⁵ ICRC Handbook (n 4) 36-38; ICRC Rules (n 35) Articles 7, 12; APEC (n 49) 12-14; USAID (n 44) 25; Faine Greenwood and others, 'The Signal Code. A Human Rights Approach to Information During Crisis' (Harvard Humanitarian Initiative 2017) 17-18 <http://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf> (The Signal Code) accessed 22 June 2018; OCHA Humanitarianism in the Age of Cyber (n 13) 11; UNHCR (n 42) 19; GDPR (n 49) Article 12, and 14; OAS Preliminary Principles (n 46) Principle 4, OECD (n 27) 15; ECOWAS (n 49) Article 38; IOM (n 1) 63-67; Oxfam (n 39) 3; WFP (n 2) 28-32; Commonwealth Model Bill (n 61) 10; AU Malabo Convention (n 60) Article 16.

3.3.2. *The Entitlement in Practice*

Information should be provided prior to the processing of the data, ideally at the moment of data collection. This may be subject to the circumstances, such as the urgency of the situation, difficulties in accessing the field, and security or logistical constraint. In such cases, the information should be made available as soon as is reasonably practical.

A list of the most common categories of information that should be provided to data subjects can be found in Box 6.¹¹⁶ Nevertheless, the amount of information that should be provided may vary depending on the circumstances. At the very least, the information should be enough to allow the data subjects to exercise effectively their entitlements to access, correction, erasure and objection.¹¹⁷

Box 6: Minimum Amount of Information

- Identity and contact details of data controller
- Purposes for the data collection and processing
- Categories of personal data collected
- With whom the data will be shared
- The rights of the data subject to access, object and rectify their personal data
- The possibilities for redress and accountability

The information should preferably be disclosed directly to the individuals concerned.¹¹⁸ However, when this is not possible, the information could be provided collectively.

When using drones to collect data from areas difficult to access, data controllers would not directly interact with data subjects. Therefore, information could not be provided directly to them. Under such circumstances, data controllers should consider other means to make the information available and accessible to the data subjects, such as by way of local communication channels.

119

Box 7: Means and Methods to Provide Information to Data Subjects

- Information published online, such as on the organization's website or on social media
- Radio, television and press
- Leaflets, posters and flyers distributed in public spaces such as markets, schools, hospitals and places of worship
- Open discussion and communication with community leaders, representatives and authorities

¹¹⁶ ICRC Rules (n 35) Article 7; APEC (n 49) 12; ICRC Handbook (n 4) 37; UNHCR (n 42) 19; WFP (n 2) 29; GDPR (n 49) Article 14; AU Malabo Convention (n 60) Article 16.

¹¹⁷ ICRC Handbook (n 4) 36-38.

¹¹⁸ *ibid.*

¹¹⁹ *ibid.* 90-91.

The information provided has to be clear, and easy for the data subjects to understand and access. Data controllers should thus consider local channels of communication for disseminating information. Box 7¹²⁰ (above) includes some of the means or methods that data controllers could use in order to provide information. Box 8¹²¹ (below) highlights some of the considerations that data controllers should bear in mind when communicating with data subjects. For instance, data controllers should consider ‘offline’ and ‘low-tech’ ways to provide information in order to ensure that data subjects with low technological access can also exercise their entitlement to information.¹²²

Box 8: How to Communicate with Data Subjects		
Information should be:	Take into account:	Use:
1) Clear	<ul style="list-style-type: none"> • Cultural and social context • Level of literacy • Language 	<ul style="list-style-type: none"> • Plain language • Concise explanation • Non-technical terminology
2) Accessible	<ul style="list-style-type: none"> • Cultural and social context • Technological access 	<ul style="list-style-type: none"> • Local channels of communication • Both on-line and off-line/ low tech

3.4. Access

3.4.1. Definition

Data subjects are entitled to access to their own personal data.¹²³

3.4.2. The Entitlement in Practice

All data subjects are entitled to access their personal data at any time, and data controllers should respond to access requests without undue delay. The entitlement to access should be easy to exercise and should not involve a complex legal process or similar measures.¹²⁴

The entitlement to access, although considered a central aspect of responsible approach to data, is not absolute.¹²⁵ Data controllers should not automatically disclose personal information to any individual requesting access to it.¹²⁶ Access should be granted only insofar as it does not frustrate the specified purposes for which personal data are collected and processed.¹²⁷ Data controllers should also exercise

¹²⁰ *ibid.* 80.

¹²¹ GDPR (n 49) Article 12; OCHA Humanitarianism in the Age of Cyber (n 13) 18.

¹²² OCHA Humanitarianism in the Age of Cyber (n 13) 18.

¹²³ IOM (n 1) 63-67; OCHA Humanitarianism in the Age of Cyber (n 13) 11; ICRC Handbook (n 4) 38-39; GDPR (n 49) Article 15; APEC (n 49) 22-28; ICRC Rules (n 35) 12-13; The Signal Code (n 115) 19; USAID (n 44) 22-23; UNHCR (n 42) 20; OECD (n 27) 58; OAS Preliminary Principles (n 46) Principle 9; ECOWAS (n 49) Article 39; WFP (n 2) 28-32; Commonwealth Model Bill (n 61) 17-19; AU Malabo Convention (n 60) Article 17.

¹²⁴ OECD (n 27) 58.

¹²⁵ OECD (n 27) 58; APEC (n 49) 22.

¹²⁶ IOM (n 1) 65.

¹²⁷ *ibid.* See principle on purpose limitation in chapter 4.

caution, taking into account the circumstances surrounding the access request on a case-by-case basis. Some of these considerations identified by a number of organizations are listed in Box 9.¹²⁸

Box 9: Considerations before Disclosing Information after an Access Request

- The best interests of the data subject
- Absence of coercion and fraud
- Proof of identification of the data subject
- Environmental factors
- Security constraints
- Potential impact on the rights and interests of other data subjects
- Public interests
- Safety of the organization's staff and individuals representing authorized third parties
- Specified purpose for which personal data are collected and processed

If, after assessing the considerations in Box 9 (above), the data controller decides that a denial of access is clearly justified, the data subject should be appropriately informed as to the reasons for such a denial.¹²⁹ Data controllers should also inform the data subject about whether they can challenge that denial, and if so, how to challenge it.¹³⁰

Data subjects should, at least, be able to obtain confirmation as to whether or not personal data concerning them has been, is being, or will be, processed. Regarding what data should be provided, the IOM states that they should only reveal personal data on a need-to-know basis, in order to meet the purpose of the access request.¹³¹ The level of disclosure will depend on an internal assessment, taking into account the abovementioned considerations. In any case, data controllers should maintain a record of access requests and the categories of personal data disclosed.

In order to meet a data subject's request to access aerial photography collected by drones, an organization may require the blurring of other faces or personal data not related to the applicant.

132

¹²⁸ IOM (n 1) 65-66; ICRC Handbook (n 4) 38-39; GDPR (n 49) Article 23; APEC (n 49) 23; ICRC Rules (n 35) Article 8(4).

¹²⁹ IOM (n 1) 66; The Signal Code (n 115) 19.

¹³⁰ APEC (n 49) 24.

¹³¹ IOM (n 1) 66.

¹³² ICRC Handbook (n 4) 93.

In the aftermath of a conflict, data controllers should exercise caution when deciding what data to disclose, as in unstable environments information could be used to harm data subjects and result in violence, such as xenophobic attacks. According to the ICRC, “data should be submitted to parties to an armed conflict [...] only after confirmation, through an ‘impact assessment’ analysis [...] that handing over this information is unlikely to give rise to disproportionate risks to the data subject’s personal security or to that of his or her family or community”. For instance, in those circumstances, brief oral summaries could be provided to fulfil the access requests.

133

Data subjects wishing to exercise their entitlement to access should provide a satisfactory proof of identification. According to the IOM, in circumstances where formal identification documents are not available (such as during a humanitarian crisis) registration cards or informal identification would suffice.¹³⁴

Access to children’s personal information can be granted to parents or legal guardians, unless the organization has sufficient reason to believe that such a request would be contrary to the interests of the child.¹³⁵ Under special circumstances, family members can also request access to the data of the data subject. In such cases, an organization should strive to balance the interest of the family members with the entitlement to privacy of the data subject.

Family members seeking family reunification may inquire about the whereabouts and well-being of a data subject. The IOM states that only non-personal data should be disclosed to family members, unless the data subject has provided consent to the disclosure of personal information. According to the IOM, in the absence of consent, and if there are no security risks, disclosure to family members should be limited to the fact that the person has been registered with the organization.

136

3.5. Correction

3.5.1. Definition

Data subjects are entitled to request that a data controller rectifies any mistakes or inaccuracies in the personal data relating to them.¹³⁷

3.5.2. The Entitlement in Practice

¹³³ IOM (n 1) 66; ICRC Rules (n 35) Article 8(3).

¹³⁴ *ibid.*

¹³⁵ IOM (n 1) 67; ICRC Handbook (n 4) 39; UNHCR (n 42) 20; ICRC Rules (n 35) Article 13.

¹³⁶ IOM (n 1) 67.

¹³⁷ GDPR (n 49) Article 16; ICRC Rules (n 35) 13; ICRC Handbook (n 4) 40; UNHCR (n 42) 20; OCHA Humanitarianism in the Age of Cyber (n 13) 11; OAS Preliminary Principles (n 46) 16; APEC (n 49) 22; WFP (n 2) 16; IOM (n 1) 66; Commonwealth Model Bill (n 61) 20; ECOWAS (n 49) Article 41; AU Malabo Convention (n 60) Article 19; CoE Convention 108 (n 69) Article 9(1)(e); OECD (n 27) 15; USAID (n 44) 9.

Procedures should be put in place¹³⁸ to allow data subjects to challenge the accuracy of data held about them¹³⁹ and correct any inaccurate data, or update any incomplete data, by providing supplementary data, for instance.¹⁴⁰ Data subjects should be notified (by distributing pamphlets, publishing notices online or orally) of their entitlement to correction, and organizations could implement the entitlement to correction by instructing data subjects to supplement, change or rectify their personal data within a defined period.¹⁴¹

As with the entitlement to access, organizations should receive satisfactory proof of identity before carrying out any correction on behalf of a data subject.¹⁴² In addition, organizations should request proof relating to the inaccuracy or incompleteness and assess the credibility of the assertion prior to granting the request for rectification.¹⁴³ However, when the request involves simply factual data (such as a request for the correction of the spelling of a name, the change of an address or telephone number), proof of inaccuracy may not be crucial.¹⁴⁴ In any case, demands for proof should not place an unreasonable burden on the data subject, to the extent that they are precluded from having the data held about them corrected.¹⁴⁵

The ICRC has identified a number of exceptions to the entitlement to correction, as outlined in Box 10.¹⁴⁶

Box 10: Exceptions to the Entitlement to Correction

- The identity of the data subject cannot be verified
- The data subject is unable to provide sufficient proof of the inaccuracy of the data
- The data are contained in a record held in the archives (in this case, a note may be included in the relevant archive file to indicate that a correction request has been made)

In certain circumstances, it may be impossible, impracticable or unnecessary to correct data.¹⁴⁷ If a request for correction is denied, the data subject should be provided with the reasons as to why, and be able to challenge such a denial.¹⁴⁸

¹³⁸ WFP (n 2) 29, 32.

¹³⁹ APEC (n 49) 22.

¹⁴⁰ ICRC Handbook (n 4) 40; GDPR (n 49) Article 16.

¹⁴¹ IOM (n 1) 36.

¹⁴² ICRC Handbook (n 4) 40.

¹⁴³ UNHCR (n 42) 20; ICRC Handbook (n 4) 40.

¹⁴⁴ ICRC Handbook (n 4) 40.

¹⁴⁵ *ibid.*

¹⁴⁶ ICRC Rules (n 35) 13.

¹⁴⁷ APEC (n 49) 25.

¹⁴⁸ APEC (n 49) 24.

During the process of data correction, access to the data may be blocked or the data controller may indicate that the data are under revision and should not be disclosed to third parties during this time.¹⁴⁹ Once the correction is made, any third parties with whom the data has been shared should be notified.¹⁵⁰

3.6. Erasure

3.6.1. Definition

Data subjects are entitled to have their personal data deleted if the continued processing of those data is not justified.¹⁵¹

3.6.2. The Entitlement in Practice

Procedures should be put in place¹⁵² to allow data subjects to have their personal data erased where:

- the data are no longer necessary, or are excessive, in relation to the original purpose(s) for which they were collected or (further) processed, and no new legitimate purpose exists;
- the data subject withdraws their consent, and there is no other basis for the processing of the data;
- the data subject successfully exercises their entitlement to object to the processing of their data, and there are no overriding grounds to continue the processing; or
- the processing does not comply with the applicable data protection and privacy laws, regulations and policies.¹⁵³

If the request for erasure meets one of these conditions and is therefore reasonable, the data controller should delete the data as requested.¹⁵⁴ The data controller should also notify any third parties with whom the data has been shared of the deletion.¹⁵⁵

However, the entitlement to erasure may be restricted and, as such, personal data will continue to be retained (subject to appropriate safeguards and taking into account the risks for and interests of the data subject), in the following circumstances:

- when erasing personal data would harm the data subject's vital interests, rights and freedoms, or those of other individuals (if, for example, an organization is concerned that the data subject is requesting erasure because of external pressure from a third party);

¹⁴⁹ OAS Preliminary Principles (n 46) 16.

¹⁵⁰ OAS Preliminary Principles (n 46) 16; IOM (n 1) 66.

¹⁵¹ GDPR (n 49) Article 17; ICRC Rules (n 35) 13; ICRC Handbook (n 4) 40; UNHCR (n 42) 20; OAS Preliminary Principles (n 46) 16; WFP (n 2) 16; IOM (n 1) 66; APEC (n 49) 22; Commonwealth Model Bill (n 61) 6; AU Malabo Convention (n 60) Article 19; ECOWAS (n 49) Article 41; CoE Convention 108 (n 69) Article 9(1)(e); OECD (n 27) 15; MSF (n 37) 13; WFP (n 2) 16.

¹⁵² WFP (n 2) 29, 32.

¹⁵³ GDPR (n 49) Article 17; ICRC Handbook (n 4) 40. See also OAS Preliminary Principles (n 46) 16.

¹⁵⁴ OAS Preliminary Principles (n 46) 16.

¹⁵⁵ OAS Preliminary Principles (n 46) 16.

- for reasons connected to the right to freedom of expression/freedom of information (including for the purposes of documenting the activities of the organization);
- when it serves the public interest to do so;
- for legitimate historical, statistical, research or scientific purposes (such as an interest in maintaining the archives that represent the common heritage of humanity);
- for long-term humanitarian purposes or to establish accountability (such as the documentation of alleged violations of international humanitarian or human rights law); or
- for the establishment, exercise or defence of legal claims.¹⁵⁶

According to the OAS, in some cases it may not be technically possible to delete all data (such as where data are replicated across multiple servers, some of which may not be under the control of the data controller) and deletions should therefore extend to those that are commercially reasonable.¹⁵⁷

As with the entitlements to access and correction, organizations should receive satisfactory proof of identity before carrying out any erasure.¹⁵⁸ However, the WFP indicates that, unlike correction, the deletion of personal data does not require that the data subject provides a justification.¹⁵⁹ According to the WFP, this is known as the ‘right to be forgotten’.¹⁶⁰ As with the entitlement to correction, while the deletion process is underway, the data controller may block access to the data or indicate that it is under revision to prevent it from being shared with third parties.¹⁶¹

3.7. Objection

3.7.1. Definition

Data subjects are entitled to object, on grounds relating their specific situation, to the processing of their personal data.¹⁶²

3.7.2. The Entitlement in Practice

Data subjects can only object to the processing of their own data. As such, as with the entitlements to access, correction and erasure, data controllers should be satisfied with the proof of identity of the individual.

¹⁵⁶ ICRC Rules (n 35) 13; ICRC Handbook (n 4) 40.

¹⁵⁷ OAS Preliminary Principles (n 46) 16.

¹⁵⁸ ICRC Handbook (n 4) 40.

¹⁵⁹ WFP (n 2) 16.

¹⁶⁰ *ibid.* See also GDPR (n 49) Article 17.

¹⁶¹ OAS Preliminary Principles (n 46) 16.

¹⁶² GDPR (n 49) Article 21; ICRC Rules (n 35) Article 11; ICRC Handbook (n 4) 40-41; UNHCR (n 42) 20; OAS Preliminary Principles (n 46) 16-17; ECOWAS (n 49) Article 40; OCHA Humanitarianism in the Age of Cyber (n 13) 11; AU Malabo Convention (n 60) Article 18.

When a data subject objects, the data controller should no longer process the personal data of the objector, unless there are compelling legitimate grounds for the processing which outweigh the entitlements of the data subject.¹⁶³ For instance, the ICRC identifies the need to document alleged violations of international humanitarian law or human rights law as a legitimate justification to continue to process data despite an objection.¹⁶⁴ Similarly, the UNHCR identifies the need of pursuing the organization's mandate.¹⁶⁵ The EU GDPR additionally recognises the grounds of scientific or historical research purposes, or statistical purposes.¹⁶⁶ Data controllers may therefore continue data processing, subject to appropriate safeguards, when this constitutes a necessary and proportionate measure to ensure one of these identified legitimate grounds.¹⁶⁷

In any case, data controllers should, as a bare minimum, take into account the risks to, and the interests of, the data subject. If a data controller decides to continue processing the data, the data subject should be appropriately informed of this decision, as well as whether there are any mechanisms to seek a review or challenge it.¹⁶⁸

3.8. Participation

3.8.1. Definition

Relevant population groups are entitled to be involved in data processing exercises, including planning, data collection, dissemination and analysis of data.¹⁶⁹

3.8.2. The Entitlement in Practice

Participation entails the exercise of all the entitlements discussed above.¹⁷⁰ This means that all individuals should be involved in decision-making processes that affect them.¹⁷¹ This should be considered throughout the entire data lifecycle: from strategic planning to data collection, analysis, interpretation, dissemination and storage.¹⁷²

¹⁶³ GDPR (n 49) Article 21; ICRC Rules (n 35) Article 11; ICRC Handbook (n 4) 41.

¹⁶⁴ ICRC Handbook (n 4) 41.

¹⁶⁵ UNHCR (n 42) 23.

¹⁶⁶ GDPR (n 49) Article 21.

¹⁶⁷ UNHCR (n 42) 20.

¹⁶⁸ ICRC Handbook (n 4) 41.

¹⁶⁹ AU Malabo Convention (n 60) 10; GDPR (n 49) preamble consideration 129; OECD (n 27) 15; IOM (n 1) 44-45; Oxfam (n 39) 2; OHCHR (n 38) 5; WFP (n 2) 16.

¹⁷⁰ WFP (n 2) 16.

¹⁷¹ OECD (n 27) 15; Sanae Fujita, *The World Bank, Asian Development Bank and Human Rights: Developing Standards of Transparency, Participation and Accountability* (Edward Elgar Publishing 2013) 147 and 153-156.

¹⁷² OHCHR (n 38) 5.

For participation to be given full effect, data controllers should include local stakeholders in every facet of the development and data collection process, ensuring that they understand and have the capacity to make decisions about the way their data is being handled, and respecting the entitlement of the local population to deny a data collection project.¹⁷³ Participation entitles both children and adults to express their views in all matters affecting them. These views should be heard and given due weight according to the age and maturity of the data subject.¹⁷⁴ Data controllers should predetermine which communities they seek to involve in a given project, to be able to set clear criteria for inclusion.¹⁷⁵

2.8.2.1. Means of Participation

All data collection exercises should include means for free, active and meaningful participation of the relevant stakeholders, in particular the most marginalised population groups.¹⁷⁶ Data controllers should therefore consider a range of procedures that facilitate and encourage participation.¹⁷⁷

The form of participation should be decided on a case-by-case basis.¹⁷⁸ Long-distance or remote options may include online consultations, appropriately publicised to ensure relevant groups are aware of the consultation process.¹⁷⁹ In this regard, it might be helpful to create advisory groups to facilitate regular engagement with vulnerable groups so that they can share feedback on the participation methods used.¹⁸⁰ On the other hand, for data controllers in the field, options may include public meetings (at locations that are easily accessible for vulnerable groups, with appropriate publicity to encourage participation) or community visits (which may incorporate public meetings, meetings with key stakeholders and representatives, and discussion with community members about issues relevant to data collection).¹⁸¹

¹⁷³ Global Initiative for Economic, Social and Cultural Rights, 'A GI-ESCR Practitioner's Guide' (Global Initiative for Economic, Social and Cultural Rights 2014) 1 <<http://globalinitiative-escr.org/wp-content/uploads/2014/05/GI-ESCR-Practitioners-Guide-on-Right-to-Participation.pdf>> accessed 21 June 2018.

¹⁷⁴ UNICEF, 'Fact Sheet: The Right to Participation' (UNICEF) <www.unicef.org/crc/files/Right-to-Participation.pdf> accessed 21 June 2018; Katie Schenk and Jan Williamson, *Ethical Approaches to Gathering Information from Children and Adolescents in International Settings: Guidelines and Resources* (Population Council 2005) 2 and 5 <www.popcouncil.org/uploads/pdfs/horizons/childrenethics.pdf> accessed 21 June 2018.

¹⁷⁵ Katie Schenk and Jan Williamson (n 174) 19.

¹⁷⁶ OHCHR (n 38) 5.

¹⁷⁷ *ibid.*

¹⁷⁸ World Bank, 'Community Involvement and the Role of Nongovernmental Organizations in Environmental Assessment' (World Bank 1999) 4 <<http://siteresources.worldbank.org/INTSAFEPOL/1142947-1118039086869/20526287/Chapter7CommunityInvolvementAndTheRoleOfNGOsInEA.pdf>> accessed 21 June 2018; OHCHR (n 38)

6.

¹⁷⁹ OHCHR (n 38) 6.

¹⁸⁰ *Ibid* 7.

¹⁸¹ *ibid.*

Participatory approaches should also be designed to ensure that information gathering supports inclusion of minority voices (such as those with disabilities), is non-discriminatory, and is age-appropriate.¹⁸² Furthermore, a participatory approach should include equal participation of women and men and adopt a gender perspective throughout its process.¹⁸³ Consequently, data controllers should take into account the relationship between women and men based on socially or culturally constructed and defined identities, statuses, roles and responsibilities that may have been assigned to one or the other sex.¹⁸⁴

2.8.2.2. Vulnerable Groups

Nearly every community has a group of people that are, for whatever intentional or unintentional reason, marginalised and unrepresented.¹⁸⁵ Data controllers should therefore ensure that the views of vulnerable or marginalised groups, and groups who are at risk of discrimination, are represented.¹⁸⁶ The terms 'vulnerability' or 'vulnerable groups' are commonly used, but often with different meanings by different practitioners.¹⁸⁷ However, almost all definitions agree that vulnerable populations are defined as those who have a greater probability than the population as a whole of being harmed and experiencing an impaired quality of life because of social, environmental, health, or economic conditions or policies.¹⁸⁸ Vulnerability is thus the degree to which a person is exposed to risk, multiplied by their lack of ability to cope or adapt.¹⁸⁹

Box 11: Examples of Vulnerable Groups¹⁹⁰

- | | |
|--|--|
| <ul style="list-style-type: none"> • Migrants • Sex workers • Homeless persons • Older persons • Refugees • HIV patients | <ul style="list-style-type: none"> • Women • Children • Indigenous peoples • Minorities • Persons with disabilities • Members of the LGBT+ community |
|--|--|

¹⁸² Katie Schenk and Jan Williamson (n 174) 5.

¹⁸³ ACAPS, *Humanitarian Needs Assessment: The Good Enough Guide* (Emergency Capacity Building Project and Practical Action Publishing 2014) 9; OHCHR (n 38) 7-8.

¹⁸⁴ OHCHR (n 38) 5.

¹⁸⁵ IFRC, 'Community early warning systems: guiding principles' (IFRC 2012) 44 <www.ifrc.org/PageFiles/103323/1227800-IFRC-CEWS-Guiding-Principles-EN.pdf> accessed 21 June 2018; Gabrielle Berman and others, 'What We Know About Ethical Research Involving Children in Humanitarian Settings: An overview of principles, the literature and case studies' (Innocenti Working Paper, UNICEF 2016) 11 <www.unicef-irc.org/publications/849-what-we-know-about-ethical-research-involving-children-in-humanitarian-settings-an.html> accessed 21 June 2018; Global Initiative for Economic, Social and Cultural Rights (n 173) 4.

¹⁸⁶ Amy Ellard-Gray and others, 'Finding the Hidden Participant: Solutions for Recruiting Hidden, Hard-to-Reach, and Vulnerable Populations' (2015) 10 *International Journal of Qualitative Methods* 1; Global Initiative for Economic, Social and Cultural Rights (n 173) 4; ACAPS (n 183) 9; OHCHR (n 38) 5.

¹⁸⁷ Johannes G Hoogeveen and others, 'A Guide to the Analysis of Risk, Vulnerability and Vulnerable Groups' (2004) Researchgate 4 <www.researchgate.net/publication/238528462_A_Guide_to_the_Analysis_of_Risk_Vulnerability_and_Vulnerable_Groups> accessed 21 June 2018.

¹⁸⁸ Robert L Barker, *The Social Work Dictionary* (National Association of Social Work 1995) 404; Jack Rothman, *Practice with Highly Vulnerable Clients* (Prentice-Hall 1994) 5-8.

¹⁸⁹ ICRC, 'Acquiring and Analysing Data in Support of Evidence-based Decisions: A Guide for Humanitarian Work' (ICRC 2017) 18 and 249 <www.icrc.org/en/publication/acquiring-and-analysing-data-support-evidence-based-decisions-guide-humanitarian-work> accessed 21 June 2018 (ICRC Acquiring and Analysing Data).

¹⁹⁰ OHCHR (n 38) 7.

However, it may be impossible or inappropriate to engage directly with certain groups.¹⁹¹ This may be the case where there are physical barriers such as a natural disaster, or when social stigma and negative stereotypes create negative ramifications for publicly identifying with a group or organization.¹⁹² Another instance could be that the group is so marginalised and/or disadvantaged that they lack the access, ability or resources to engage productively in participatory processes.¹⁹³

2.8.2.3. Identifying Relevant and Vulnerable Groups

To facilitate participation of the relevant individuals and population groups, it is necessary to identify the vulnerable groups.¹⁹⁴ Identifying vulnerable groups can be done proactively through discussion with national human rights institutions (NHRIs), NGOs and other relevant experts.¹⁹⁵ The OCHR has stated that, where appropriate, NGOs, NHRIs and other representatives of relevant stakeholders should participate on behalf of these groups to provide relevant perspectives and information (provided they are competent to represent the group's interests).¹⁹⁶

3.9. Concluding Remarks

The entitlements of data subjects identified for the purposes of this report, namely privacy, information, access, correction, erasure, objection, and participation have each been defined, followed by an explanation of the substance of the entitlement and guidance for its implementation in practice.

While each of the entitlements identified is individually important, as has been seen (and will continue to be discussed in chapter 4), they are not all absolute, and may be limited in certain circumstances. Moreover, guidelines explicitly identifying practical mechanisms to allow for these entitlements to be fully exercised are still lacking. This point will be further addressed in chapter 5 regarding remaining challenges in this field.

¹⁹¹ Lynn Wolfrey (n 307) 4.

¹⁹² OHCHR (n 38) 5-6.

¹⁹³ *ibid.*

¹⁹⁴ A vulnerability analysis normally starts by defining vulnerability in a given context (for instance, defining that which the groups are vulnerable to) and then identifies specific criteria, known as domains: ICRC, 'Acquiring and Analysing Data in Support of Evidence-based Decisions: A Guide for Humanitarian Work' (n 189) 18 and 249; Lotsmart Fonjong, 'Fostering women's participation in development through non-governmental efforts in Cameroon' (2001) 3 *The Geographical Journal* 223; Amazon Watch, 'The Right to Decide: the importance of respecting free, prior, and informed consent' (2011) <<http://amazonwatch.org/assets/files/fpic-the-right-to-decide.pdf>> accessed 22 June 2018; David Burfoot, 'Children and young people's participation, Arguing for a better future' (2003) 3 *Youth Studies Australia* 44; Constanza Tabbush, 'The elephant in the room': silencing everyday violence in rights-based approaches to women's community participation in Argentina (2010) 3 *Community Development Journal* 325.

¹⁹⁵ This entails including relevant NGO's in thematic or advisory boards or committees convened by the data controller and establishing focal points within data collection organizations who are responsible for seeking information and perspectives from groups of interest; OHCHR (n 38) 5-6.

¹⁹⁶ Global Initiative for Economic, Social and Cultural Rights (n 173) 5; OHCHR (n 38) 6.

4. DATA PROTECTION PRINCIPLES

4.1. Introduction

For the purposes of this report, a number of data protection principles have been identified, namely legitimate processing, informed consent, purpose limitation, data minimisation, storage limitation, data quality, transparency and openness, data security, and accountability. These principles (which identify considerations that should be taken into account at every stage of the data lifecycle), are addressed to organizations collecting and processing data, and should form part of any responsible approach to data protection. Proportionality has been identified by some organizations as an additional principle to those already mentioned. However, for the purposes of the report, proportionality has not been included as a principle in itself, but is instead deemed to be an important consideration when interpreting and implementing the principles. At every stage of the data lifecycle, a proportionality assessment should be conducted to ensure that any “particular action or measure related to the [p]rocessing of [p]ersonal [d]ata is appropriate to its pursued aim”.¹⁹⁷ Proportionality considerations also aim to ensure that any potential risks and harms to data subjects are not excessive in relation to the perceived benefits of action taken in collecting and processing data.¹⁹⁸

Robust data protection policies, based on the principles for responsible data processing set out in this chapter, should be developed and followed by all actors processing data. As set out in chapter 2, a number of countries have implemented data protection legislation at the national level, which can protect data subjects against the actions of private persons and the state. In some regions, a human right to data protection is even recognised.¹⁹⁹ However, a number of countries have very loose legislation, or none at all. Although not universally legally binding, data protection *guidelines* can offer the requisite protection to data subjects to safeguard their human dignity. It is therefore crucial for individual organizations processing data to establish and follow such guidelines, even where there is no legal obligation to do so.

Even where national data protection legislation has been implemented, some organizations, namely international organizations enjoying privileges and immunities, are not subject to national legislation,²⁰⁰ and the implementation of data protection standards may not be a legal obligation.²⁰¹ Nevertheless, it is still in

¹⁹⁷ ICRC Handbook (n 4) 26.

¹⁹⁸ UNHCR (n 42) 16; UNDG (n 40) 5; UN Global Pulse Big Data (n 41) 11; IOM (n 1) 143; MSF (n 37) 5; ICRC Handbook (n 4) 26.

¹⁹⁹ The European Court of Human Rights (ECtHR) has interpreted Article 8 of the ECHR (covering the right to privacy) to also give rise to a right of data protection. See e.g. *Amann v Switzerland*, no 27798/95, ECHR 2000-II, para. 65. The right to protection of personal data is also recognised under Article 8 of the Charter of Fundamental Rights of the European Union (adopted 12 December 2007, entered into force December 2009), in addition to the right to private and family life under Article 7. This is also evidenced by the wording of Article 1 of the CoE Convention 108.

²⁰⁰ This could also apply to some regional instruments with direct effect, such as the GDPR.

²⁰¹ This consideration also applies to the entitlements of data subjects.

the interests of such organizations to establish and implement data protection policies, and this may be a prerequisite for them to receive data from other entities.²⁰²

The principles identified for the purposes of this report are each individually important, ensuring operational efficiency for the organizations implementing them by: preserving the trust and confidence of data subjects in the organization; reducing cost; and improving the timeliness of data collection and processing. However, since humanitarian and development organizations often operate in exceptional emergency circumstances, a certain degree of flexibility is sometimes required when applying the principles identified in this report.²⁰³ When this is the case concerning an individual principle, it will be explicitly mentioned in the relevant section. Moreover, “as new types of data are being discovered and used, new risks [to data subjects] and types of harm may arise.”²⁰⁴ Therefore, given these prospective technological advances, the principles identified in this report may evolve over time, and any data protection policies established should be considered as ‘living instruments’, which may require to be amended in the future.²⁰⁵

In this chapter, the principles of legitimate processing, informed consent, purpose limitation, data minimisation, storage limitation, data quality, transparency and openness, data security, and accountability will first each be defined, followed by an explanation of the substance of the principle, and guidance for its implementation in practice.

4.2. Legitimate Processing

4.2.1. Definition

Personal data should only be processed on a legitimate basis.²⁰⁶

4.2.2. Substance

In order to process data, organizations are required to establish a legitimate basis. Box 12²⁰⁷ sets out the possible legitimate bases for data processing.

²⁰² ICRC Handbook (n 4) 16.

²⁰³ ICRC Handbook (n 4) 17; IOM (n 1) 9.

²⁰⁴ UN Global Pulse Big Data (n 41) 8.

²⁰⁵ UNDG (n 40) 3.

²⁰⁶ GDPR (n 49) Article 5(1)(a); ICRC Handbook (n 4) 25; WFP (n 2) 16; OAS, 9; IOM (n 1) 19; OCHA Humanitarianism in the Age of Cyber (n 13) 11; UN Global Pulse Big Data (n 41) 10; OECD (n 27) 14; UNHCR (n 42) 15; APEC (n 49) 15; Commonwealth Model Bill (n 61) 10; ECOWAS (n 49) Article 24; AU Malabo Convention (n 60) Article 13, Principles 2; CoE Convention 108 (n 69) Article 5(3); UNDG (n 40) 4. This principle is also referred to as “Fair and Legitimate Processing” or “Fair and Lawful Processing” by a number of these organizations.

²⁰⁷ ICRC Handbook (n 4) 44; ICRC Rules (n 35) Article 8; UNHCR (n 42) 15; GDPR (n 49) 6.

Box 12: Legitimate Bases for Data Processing

- Consent of the data subject
- Vital interest of the data subject or another person
- Public interest
- Performance of a contract
- Compliance with a legal obligation
- Legitimate interest of the data controller (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data)

To process data on the ground of a vital interest, there must be sufficient evidence to consider that in the absence of processing, the data subject could be at risk of physical or moral harm.²⁰⁸ For the ground of public interest, the processing must fall under within mandate of the organization established under national, regional or international law.²⁰⁹

When new technology and data sources (such as social media data, mobile phone data, or financial transaction data) are used, organizations sometimes do not collect the data themselves, but receive data from other sources and then process it.²¹⁰ Even if an organization does not collect the data itself, it should still exercise due diligence and attempt to ensure that the data has been collected legitimately, including in compliance with applicable privacy norms and the highest ethical standards.²¹¹ Moreover, organizations should ensure that the data provider has the legitimate right to share the data.²¹²

Depending on which legitimate basis data are processed, certain entitlements of data subjects, namely erasure and objection, may be restricted and will not apply. See Box 13,²¹³ illustrating (by way of an 'X') when data subjects will not be able to exercise the entitlements to erasure and objection. For instance, when the legitimate basis for data processing is the ground of vital interest of the data subject or another person, the data subject will not be entitled to object to the data processing.

Box 13: Restriction of Data Subject Entitlements	Erasure	Objection
Consent		X (But entitled to withdraw consent)
Vital interest		X

²⁰⁸ ICRC Handbook (n 4) 44.

²⁰⁹ ICRC Handbook (n 4) 44.

²¹⁰ UN Global Pulse (n 41) 10.

²¹¹ *ibid.*

²¹² *ibid.*

²¹³ Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (Information Commissioner's Office 2018) <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>> accessed 22 June 2018, 53.

Public interest	X	
Performance of a contract		X
Compliance with a legal obligation	X	X
Legitimate interest		

4.2.3. The Principle in Practice

The nature of the work of the organization will influence the determination of the legitimate basis that should be used. For instance, the ICRC usually works in areas of armed conflict and high instability. As a result, it has stated that, “while the organization would prefer consent to be the legitimate basis for processing data [...] in the vast majority of contexts where the ICRC works [...] consent is not the most feasible basis for processing.”²¹⁴ This occurs very often in situations of humanitarian crisis, where other considerations such as the urgency of the situation may force organizations to rely on a legitimate basis that is not consent.²¹⁵ The method used for data collection will also influence the suitability of consent. This is especially relevant regarding new technologies for data collection. For example, when collecting data using remote methods such as satellite imagery, it might not be possible to obtain consent.²¹⁶

In 2016, the United Kingdom Information Commissioner’s Office (ICO) issued monetary penalties for two charities, the Royal Society for the Prevention of Cruelty to Animals and the British Heart Foundation, for having secretly performed assessments of the wealth of millions of donors and shared such data with other organizations without the knowledge or legitimate expectations of the data subjects. The ICO set out that, as consent cannot be inferred, there was no legitimate basis on which to process the data (as none of the other legitimate bases for processing data applied).

217

4.3. Informed Consent

4.3.1. Definition

Data subjects should agree to the processing of their personal data by providing consent, which must be obtained voluntarily and with full knowledge of all the relevant implications.²¹⁸

4.3.2. Substance

²¹⁴ ICRC Acquiring and Analysing Data (n 189), 63.

²¹⁵ OCHA Humanitarianism in the Age of Cyber (n 13) 11.

²¹⁶ *ibid.*

²¹⁷ Tim Gough, Gough T, ‘Fair and lawful processing: a hard lesson for charities, and what to do next (*Linkedin*, 9 December 2016) <www.linkedin.com/pulse/fair-lawful-processing-hard-lesson-charities-what-do-next-tim-gough> accessed 21 June 2018.

²¹⁸ IOM (n 1) 41-48; ICRC (n 4) 45-48; ICRC Acquiring and Analysing Data (n 189), 62-63; ICRC Rules (n 35) Article 1; UNHCR (n 42) 9; OCHA Humanitarianism in the Age of Cyber (n 13) 10; GDPR (n 49) Article 7; APEC (n 49) 15-20; OECD (n 27) 14; ECOWAS (n 49) Article 23; OAS Preliminary Principles (n 46) 8-9; WFP (n 2) 46-55; UNDG (n 40) 8; Commonwealth Model Bill (n 61) 10; AU Malabo Convention (n 60) Article 13(1).

For consent to be genuine, it has to be voluntary, with comprehension of the relevant implications, and it must be given by a person who has the capacity to consent. It is important to bear in mind that obtaining consent may also amount to a legal obligation in some jurisdictions. For instance, one of the major changes introduced by the EU GDPR is the strict legal conditions in order for consent to be valid.²¹⁹

4.3.2.1. Voluntariness

Consent must be given voluntarily and unambiguously.²²⁰ This would normally take the form of a written, or if not possible, an oral, statement, or any other clear affirmative action.²²¹ Voluntariness implies that the consent is given free of any coercion or inflated promise.

Consent would not be considered freely given if the process of obtaining it involve people who have power over the participants, or if there were a clear imbalance between the data controller and the data subject (such as if the data controller were a public authority).²²² In addition, the EU GDPR states that consent would be presumed to have not been freely given if the performance of a contract (including the provision of a service) is dependent on the consent, despite such consent not being necessary for such performance.²²³

4.3.2.2. Comprehension

Consent can be said to be 'informed' when the data subject has all the relevant information regarding the possible risks and/or implications involved in the data processing and still consents to it. The ability to consent is dependent on the quality of the information given.²²⁴ The information provided should thus be clear and accessible.²²⁵ This may be challenging when obtaining consent through digital (i.e. non-face-to-face) environments. When consent is obtained through an online registration process, very often individuals agree to the terms and conditions without actually reading them. This is why the EU GDPR explicitly states that when consent is obtained through electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which is provided.²²⁶ Additionally, if consent is given in a written declaration which also includes other matters, the request for consent should be presented in a manner clearly distinguishable from those other matters.²²⁷

²¹⁹ GDPR (n 49) Article 7.

²²⁰ OAS Preliminary Principles (n 46) 8; GDPR (n 49) Article 7; ICRC Handbook (n 4) 45.

²²¹ ICRC Handbook (n 4) 45; GDPR (n 49) Recital 32; UNHCR (n 42) 9.

²²² Responsible Data Forum (n 19) 66; GDPR (n 49) Recital 43; ICRC Handbook (n 4) 45.

²²³ GDPR (n 49) Article 7 and Recital 43.

²²⁴ UNICEF (n 104) 67.

²²⁵ See Box 6 under the entitlement to information, above, which contains the considerations that should be taken into account when communicating information to the data subjects.

²²⁶ GDPR (n 49) Recital 32.

²²⁷ GDPR (n 49) Article 7.

When genuine informed consent is difficult to obtain and the data subject may not quite reach the required level of understanding to meet the threshold of ‘informed’ consent, due to the complexities attached to the use of new technologies, the organization could consider acting on other legitimate bases.²²⁸

4.3.2.3. Capacity or Competence

The data subject has to be competent to give consent and must have the ability and capacity to comprehend the implications of giving such consent. This consideration is of particular importance regarding vulnerable groups such as children, people with mental disabilities or people who have recently being subject to significant trauma.²²⁹

4.3.3. The Principle in Practice

Data controllers should assess whether consent is the most appropriate basis for the data collection and processing. Box 14²³⁰ provides some examples of when consent may not be appropriate, as the surrounding circumstances might not allow the data subject to give free unambiguous consent. If it is not possible to obtain consent, data controllers might still be able to process data, provided that they are acting under one of the other of the legitimate bases explained in the previous section. In such cases, data controllers would still have the obligation to provide information about the data processing to the data subjects, since knowledge is the minimum requirement (see the section on the entitlement to information in chapter 3).²³¹

Box 14: Instances where Consent may not be the most Appropriate Legitimate Basis

- When data controllers are in a position of power over the data subject
- When consent is conditional to the provision of a service
- When collecting data using remote technology

Consent has to be obtained individually from each data subject. This means that the ‘consent of the community’ or the ‘consent of the authorities’ are not viable alternatives to an individual’s consent. Respect for social, cultural and religious norms may add additional constraints, and would thus have to be balanced with the need to obtain informed consent from the data subjects.²³²

²²⁸ See Box 12: Legitimate Bases for Data Processing, above.

²²⁹ For more detailed information regarding informed consent with children see UNICEF (n 104) 35-41; ICRC Handbook (n 4) 46-47; GDPR (n 49) Article 8; IOM (n 1) 46-47.

²³⁰ GDPR (n 49) Recital 43; OCHA Humanitarianism in the Age of Cyber (n 13) 10.

²³¹ OECD (n 27) 56; IOM (n 1) 41; ICRC Handbook (n 4) 37.

²³² IOM (n 1) 44.

In some special circumstances, the consent of the head of the family may be taken on behalf of the data subject. Even in such situations, organizations should take appropriate measures to inform all family members of the reasons why their personal data are being collected and processed.

233

When using drones to collect data from communities which are difficult to access, it is not sufficient for an organization to ask the leaders of the community for consent. The organization should instead use other legitimate bases in order to collect the data. For example, if drones are used for search and rescue operations, an organization could still collect the data under the legitimate basis of the vital interests of the data subjects.

234

If consent is established as the legitimate basis for data processing, data controllers should conduct a risk assessment at the planning stage, including an assessment of urgency and data sensitivity, in order to decide about the appropriate form of consent, or the amount of information that should be disclosed to the data subjects.²³⁵ The information should be sufficient to allow the data subject to make a risk assessment as to their participation in the data processing. Box 15²³⁶ includes a list of the information that should be provided in order to obtain consent.

Box 15: Information that should be provided to Obtain Informed Consent

- Identity and contact details of data controller
- Purposes for the data collection and processing
- Categories of personal data collected
- With whom the data would be shared
- The entitlements of the data subject to access, correction, erasure and objection
- The possibilities for redress and accountability
- A description of the consequences of participation, including both foreseeable risks as well as possible benefits
- How confidentiality would be ensured
- The period of time for which data would be stored

Informed consent should be obtained at the time of the collection of data, or as soon as it is reasonably practical thereafter.²³⁷ Furthermore, the form of consent used (such as whether it was given by written agreement) and its content (such as whether it allows for disclosure to third parties) should be accurately recorded and documented by the data controller.²³⁸

²³³ *ibid.*

²³⁴ ICRC Handbook (n 4) 92-93.

²³⁵ Responsible Data Forum (n 19) 69.

²³⁶ IOM (n 1) 43; WFP (n 2) 49; Responsible Data Forum (n 19) 67; ICRC Handbook (n 4) 37; GDPR (n 49) Articles 13-14.

²³⁷ IOM (n 1) 44.

²³⁸ IOM (n 1) 42; ICRC Handbook (n 4) 47; GDPR (n 49) Article 7.

Data controllers should inform the data subjects of the purpose(s) for which the data are processed. If there are several purposes, consent should be given for each of them.²³⁹ Consent should be renewed if personal data are to be processed for a purpose other than the one for which they were obtained (when the new purpose varies so much that it is incompatible with the original purpose).²⁴⁰ Therefore, it is advisable to obtain consent for additional foreseeable purposes at the time of data collection, in order to avoid the practical difficulties of obtaining consent again at a later stage.²⁴¹

Finally, as a general rule, data subjects can withdraw consent at any stage of the data processing.²⁴² Data controllers should ensure that the mechanism by which to withdraw consent is as easy to exercise as the action of giving consent was in the first place.²⁴³

4.4. Purpose Limitation

4.4.1. Definition

Personal data should be collected for specified, explicit and legitimate purposes and should not be further processed in a manner that is incompatible with those purposes.²⁴⁴

4.4.2. Substance

The purpose limitation principle tries to prevent a “functional creep”, i.e. using personal data in ways not specified in the original purpose, and therefore without the consent of the data subject.²⁴⁵

4.4.2.1. Specified and Legitimate Purpose

The purpose(s) for which personal data are collected should be specified, and known to the data subject, prior to, or at the time of, data collection.²⁴⁶ The purpose specification should be explicit, and data subjects should be provided with a clear explanation of the purpose, which should, in turn, be clearly defined,²⁴⁷ as the use of vague or very general descriptions of the purpose would not sufficiently protect the entitlements

²³⁹ GDPR (n 49) Recital 32; Oxfam (n 39) 3; IOM (n 1) 43.

²⁴⁰ OAS Preliminary Principles (n 46) 8; IOM (n 1) 43, Oxfam (n 39) 3; UNGD (n 40) 8.

²⁴¹ IOM (n 1) 43.

²⁴² GDPR (n 49) Article 7; OAS Preliminary Principles (n 46) 8; IOM (n 1) 43; Oxfam (n 39) 3.

²⁴³ GDPR (n 49) Article 7; OAS Preliminary Principles (n 46) 8; WFP (n 2) 47.

²⁴⁴ GDPR (n 49) Article 5(1)(b); IOM (n 1) 27; OECD (n 27) 14; UNHCR(n 42) 16; OCHA Humanitarianism in the Age of Cyber (n 13) 11; USAID (n 44) 8; UNHCR (n 42) 15; ICRC Rules (n 35) 8-9; Oxfam (n 38) 3; WFP (n 2) 16; OAS Preliminary Principles (n 46) 10; ICRC Handbook (n 4) 26; Commonwealth Model Bill (n 61) 10; APEC (n 49) 16; ECOWAS (n 49) Article 25; AU Malabo Convention (n 60) Article 13, Principles 3(a); CoE Convention 108 (n 69) Article 5(4)(b); UN Global Pulse Big Data (n 41) 10; MSF (n 37) 11; UNDG (n 40) 4.

²⁴⁵ IOM (n 1) 27.

²⁴⁶ IOM (n 1) 27; OECD (n 27) 14; UNHCR (n 42) 16; OCHA Humanitarianism in the Age of Cyber (n 13) 11; USAID (n 44) 8; GDPR (n 49) Article 5(1)(b).

²⁴⁷ IOM (n 1) 27; WFP (n 2) 23.

of data subjects,²⁴⁸ since the purpose would be subject to the discretionary power of users.²⁴⁹ Data subjects should also be aware of any possible *related* purpose(s) for which their personal data could be used for further processing, to ensure transparency as far as possible.²⁵⁰

However, the requirement of a specified and legitimate purpose may be restricted for a limited time in exceptional circumstances if it is necessary to do so to protect data subjects or other individuals.²⁵¹ For example, the initial purpose may need to be broad to enable a large collection of data during an emergency (since it may not be immediately possible to determine the specific needs of those affected and what assistance and programmes would be required further down the line).²⁵²

The specified purpose should also be legitimate, i.e. based on a legitimate need of the organization (such as the need to achieve the objectives and intended outcomes of its projects, which is often the organization's mandate)²⁵³ and in accordance with all relevant legal rules,²⁵⁴ which should be determined by the data controller following an internal assessment.²⁵⁵

If, due to unforeseen circumstances, the specified purpose is significantly altered, data subjects should be notified.²⁵⁶ In cases where it is impractical to contact the data subject directly, "all reasonable steps should be taken to generally communicate significant changes to the target population group, for example, through public campaigning, radio broadcast, publications on the Internet or distributing pamphlets."²⁵⁷

Personal data should only be used in accordance with the purposes determined at the time of data collection, unless the consent of the data subject is obtained or deviation is otherwise permitted by law.²⁵⁸

4.4.2.2. Legitimate Further Processing

Further processing of such data, i.e. for purposes other than those specified at the time of collection, may be permissible if it is compatible with those original purposes, including where the processing is "necessary for

²⁴⁸ Nikolaus Forgó, Stefanie Hanöld and Benjamin Shutze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), *New Technology, Big Data and the Law* (Springer 2017) 28.

²⁴⁹ WFP (n 2) 23.

²⁵⁰ ICRC Handbook (n 4) 26; IOM (n 1) 28.

²⁵¹ *ibid*, 26.

²⁵² *ibid*, 27.

²⁵³ WFP (n 2) 23.

²⁵⁴ Nikolaus Forgó, Stefanie Hanöld and Benjamin Shutze (n 248) 28.

²⁵⁵ IOM (n 1) 27.

²⁵⁶ *ibid*, 28.

²⁵⁷ *ibid*, 27.

²⁵⁸ OECD (n 27) 14; USAID (n 44) 8; IOM (n 1) 27; ICRC Rules (n 35) 8-9; Oxfam (n 39) 3; UNHCR (n 42) 15.

historical, statistical or scientific purposes.”²⁵⁹ There must be a “reasonable and direct connection” to the original purposes.²⁶⁰

A “secondary purpose that is compatible with the original purpose could be the use of personal data to continue the provision of assistance to” data subjects, or the cross-checking of registration data of one project against data of another.

261

The compatibility assessment “is particularly important in humanitarian situations, because an improperly narrow understanding of compatibility could prevent the delivery of humanitarian benefits” to data subjects.²⁶² As such, “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.”²⁶³

However (when consent is the legitimate basis for the data processing), if the purpose of the data collection changes to something incompatible with the original purpose, data subjects must be informed of the new purpose and provide their consent.²⁶⁴ In any case, further processing should be forbidden if the risks to the data subject or their family outweigh the benefits of such processing, such as a risk that the processing “may threaten their life, integrity, dignity, psychological or physical security, liberty, or their reputation.”²⁶⁵ Nevertheless, further processing should be permissible, in theory, if it is necessary “to safeguard public security and the lives of affected individuals”, or there is another legal basis for the processing.²⁶⁶ This requires a case-by-case assessment.²⁶⁷

4.4.3. *The Principle in Practice*

4.4.3.1. *Specified and Legitimate Purpose*

In a humanitarian context, the ICRC has given a number of examples of possible specific purposes, such as:

- providing humanitarian assistance and/or services to affected populations to sustain livelihood;
- restoring family links between people separated due to humanitarian emergencies; or
- providing documentation or legal status/identify to, for instance, displaced or stateless people.²⁶⁸

²⁵⁹ ICRC Rules (n 35) 9; GDPR (n 49) Article 5(1)(b).

²⁶⁰ IOM (n 1) 28.

²⁶¹ WFP (n 2) 24.

²⁶² ICRC Handbook (n 4) 30.

²⁶³ ICRC Handbook (n 4) 31.

²⁶⁴ WFP (n 2) 24.

²⁶⁵ ICRC Handbook (n 4) 30; ICRC Rules (n 35) 9. This is a proportionality assessment.

²⁶⁶ ICRC Handbook (n 4) 30.

²⁶⁷ *ibid.*

²⁶⁸ ICRC Handbook (n 4) 26.

The principle of purpose limitation can often be challenged in practice by data *sharing*, especially if the principle of data minimisation is also ignored.²⁶⁹ Data sharing should therefore be “efficient” (improving the quality and value of research), avoid any unnecessary duplication, and be proportionate.²⁷⁰ Moreover, data should only be shared with the consent of the data subject, for the specified purpose, and “under the guarantee of adequate safeguards” concerning confidentiality, for instance.²⁷¹

When the UNHCR was considering whether to share biometric data, including iris scans, with the Lebanese Government, there was concern that the biometric database could be linked with another or appropriated for security or political purposes, such as sharing with the Syrian Government. Both the WFP and the IOM explicitly refer to the fact that the use of biometric data (being highly sensitive) should be limited to the specified purpose, and should never be used or shared for any purpose including, for instance, alleged national or State security measures (as this could result in, *inter alia*, unfair discrimination or limit the free and lawful movement of migrants).

272

4.4.3.2. Legitimate Further Processing

Regarding further processing, Box 16²⁷³ sets out a list of factors that should be taken into account in determining whether such processing is compatible with the original specified purpose.

Box 16: Compatibility Factors for Further Processing

- The situation in which the data were collected, including the reasonable expectations of the data subject as to their further use
- Any link between the original specified purpose and the secondary purpose
- The nature and scope of the personal data used or disclosed for the secondary purpose
- The consequences of further processing for the rights and interests of the data subject
- The extent to which appropriate safeguards would protect the confidentiality of personal data and the anonymity of the data subject

4.5. Data Minimisation

4.5.1. Definition

Personal data should be adequate, relevant and not excessive in relation to the specified purpose(s).²⁷⁴

4.5.2. Substance

²⁶⁹ Responsible Data Forum (n 19) 84.

²⁷⁰ MSF (n 37) 5; Karin Clark and others (n 102) 17; OCHA Humanitarianism in the Age of Cyber (n 13) 11.

²⁷¹ IOM (n 1) 51.

²⁷² OCHA Humanitarianism in the Age of Cyber (n 13) 11; IOM (n 1) 27; WFP (n 2) 23.

²⁷³ ICRC Handbook (n 4) 29; IOM (n 1) 28.

²⁷⁴ GDPR (n 49) Article 5(1)(c); UNHCR (n 42) 16; ICRC Handbook (n 4) 26; ICRC Rules (n 35) 9; OECD (n 27) 14; USAID (n 44) 8; Oxfam (n 39) 4; UN Global Pulse Principles (n 41); WFP (n 2) 27; OAS Preliminary Principles (n 46) 10; IOM (n 1) 35; APEC (n 49) 15; ICRC Acquiring and Analysing Data (n 189) 56; ECOWAS (n 49) Article 25(2); AU Malabo Convention (n 60) Article 13, Principle 3(b); CoE Convention 108 (n 69) Article 5(4)(c); OCHA Humanitarianism in the Age of Cyber (n 13) 16; UNDG (n 40) 6.

The collection of personal data should not be excessive and should be limited to the minimum amount that is necessary to fulfil the specified purpose(s). Data should not be collected “just in case” for future purposes that are not specified and made clear to the data subject prior to collection.²⁷⁵

However, to achieve the best results, data analytics, for instance, usually requires large data sets with as much information as possible covering a significant time period, which contradicts the principle of data minimisation.²⁷⁶ This therefore reinforces the importance of ensuring that the purpose of data collection and processing is as specific as possible.²⁷⁷

Following collection, the processing of the data should also be limited to the minimum necessary. The processing of personal data is necessary if it directly helps to achieve the purposes for which it was collected; if the purpose can be achieved through another reasonable means, the processing is not necessary.²⁷⁸ In addition, data sharing should be limited to the minimum necessary to fulfil the specified purpose(s).²⁷⁹

Oxfam staff have recognised data minimisation as being one of the most relevant principles in their work, in particular noting the importance of such a principle in unstable political contexts, such as programmes in Iraq (where they have chosen to simply take ID numbers as opposed to full hard copies of identification documents).

280

4.5.3. The Principle in Practice

The WFP has identified a number of questions that should be asked to ensure that the principle of data minimisation is respected; if an organization could answer no to any of these questions, then the data should not be collected:

- Does the organization full and clearly understand the purpose for which it is collecting data and the information requirements to fulfil that purpose?
- Is the data being collected absolutely necessary to fulfil the specified purpose?
- If an individual were to ask the organization to justify every piece of data being collected about them, could they do so?²⁸¹

²⁷⁵ WFP (n 2) 27.

²⁷⁶ ICRC Handbook (n 4) 78.

²⁷⁷ *ibid.*

²⁷⁸ OAS Preliminary Principles (n 46) 10.

²⁷⁹ WFP (n 2) 56.

²⁸⁰ The Engine Room, *Responsible Data at Oxfam: Translating Oxfam's Responsible Data Policy into practice, two years on* (The Engine Room and Oxfam 2017) <<https://oxfamlibrary.openrepository.com/oxfam/bitstream/10546/620257/1/rr-responsible-data-at-oxfam-190417-en.pdf>> accessed 22 June 2018, 4.

²⁸¹ WFP (n 2) 27.

For example, if data subjects are simply being assessed for food distributions, it may not be necessary to collect data about level of education.²⁸² In addition, if biometric data are collected for identification purposes, such data must be proportionate to these purposes.²⁸³ Therefore, only the amount of biometric data necessary for the identification of an individual should be collected, with the range of biometric data sets also limited (“collecting facial imagery or iris scans may not be considered as proportionate if photos and fingerprints are already being used for identification purposes”).²⁸⁴

Data controllers should regularly conduct assessments throughout the data lifecycle to ascertain whether personal data continue to be necessary, relevant and proportionate.²⁸⁵

4.6. Storage Limitation

4.6.1. Definition

Personal data should only be retained for as long as is necessary to achieve the specified purpose(s).²⁸⁶

4.6.2. Substance

Personal data should be destroyed or rendered anonymous as soon as the specified purpose for which it was collected and processed is achieved. Any further retention of data should be justified.²⁸⁷ Data should also be erased if a data subject withdraws their consent or successfully objects to the processing of the data.²⁸⁸

If organizations wish to retain data for additional specified purposes that are not compatible with the original specified purpose, the consent of the data subject must again be obtained.²⁸⁹ However, data may be retained beyond the fulfilment of the specified purposes if it is for the benefit of the data subject and in their best interests (extending the length of a project, for example).²⁹⁰ In this case, data controllers should:

- identify the additional specified purpose;
- define the period of further retention;
- conduct a risk-benefit assessment; and

²⁸² *ibid*, 26.

²⁸³ ICRC Handbook (n 4) 132.

²⁸⁴ ICRC Handbook (n 4) 132.

²⁸⁵ IOM (n 1) 38; ICRC Handbook (n 4) 115.

²⁸⁶ GDPR (n 49) Article 5(1)(e); UNHCR (n 42) 29; WFP (n 2) 82; ICRC Rules (n 35) 9; USAID (n 44) 21; UN Global Pulse Principles (n 41); IOM (n 1) 81; OCHA Humanitarianism in the Age of Cyber (n 13) 11; ICRC Handbook (n 4) 31; Commonwealth Model Bill (n 61) 15; ECOWAS (n 49) Article 25(3) & (4); AU Malabo Convention (n 60) Article 13, Principle 3(c) & (d); CoE Convention 108 (n 69) Article 5(4)(e); UNDG (n 40) 6.

²⁸⁷ UN Global Pulse Principles (n 41).

²⁸⁸ ICRC Handbook (n 4) 27; ICRC Rules (n 35) 9.

²⁸⁹ IOM (n 1) 82.

²⁹⁰ IOM(n 1) 82; WFP (n 2) 82.

- determine whether the data subject would reasonably expect their personal data to be used for the additional specified period.²⁹¹

Data may be retained or archived, and not destroyed, when there is a legitimate reason to do so, such as to ensure long-term provision of humanitarian services, or for historical, statistical or scientific purposes, taking into account the risks for the data subject and putting in place appropriate safeguards.²⁹² Anonymised data may also be retained for an organization's legitimate use, such as research and evaluation relating to their mandate.²⁹³ However, it must be borne in mind that anonymised data may still provide enough information to re-identify an individual by inference or through aggregation with data from other sources.²⁹⁴

According to the IOM, data controllers should be sure to carefully monitor the retention and destruction of personal data, however, because "overzealous application of the retention principle may lead to premature destruction of personal data."²⁹⁵ For example, the data subject could benefit from subsequent projects and therefore destroying the personal data would be both disproportionate to the interests of the data subject and costly to the organization.²⁹⁶

4.6.3. *The Principle in Practice*

The ICRC has devised a number of questions that should be considered in determining whether the data should be retained:

- 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?²⁹⁷

²⁹¹ IOM (n 1) 82.

²⁹² ICRC Rules (n 35) 9; ICRC Handbook (n 4) 27.

²⁹³ WFP (n 2) 82.

²⁹⁴ *ibid.*

²⁹⁵ IOM (n 1) 81.

²⁹⁶ *ibid.*, 82.

²⁹⁷ ICRC Handbook (n 4) 27-28.

Some organizations set a minimum data retention period (such as a number of months, a year, or ten years), at the end of which the data must be reviewed to determine whether their retention is still necessary to fulfil the purpose for which they were collected.²⁹⁸ The retention period may be exceeded, however, where it is necessary, for instance, in monitoring and evaluation or statistical analysis.²⁹⁹ When using drones to collect data, data collection devices should be designed to allow for a defined storage period to be set and personal data which are no longer necessary thereafter to be automatically deleted.³⁰⁰

When data are destroyed, all copies should be destroyed and reasonable steps should be taken to ensure that any third parties with which the data have been shared also destroy the data.³⁰¹ Data controllers should aim to prevent any possibility of future retrieval when destroying data, therefore, when dealing with electronic records, simply deleting records from databases or files from computers is not sufficient, and more sophisticated techniques should be used.³⁰² Data controllers should maintain disposal records including the date, time and method of destruction, as well as the nature of the data destroyed.³⁰³

Organizations should be aware, as well as informing data subjects, of the fact that some of the data entered into messaging apps, for example, are also retained and stored by third parties, i.e. the messaging app companies, which can then share some of that data with other parties.³⁰⁴

4.7. Data Quality

4.7.1. Definition

Personal data should be accurate, complete and kept up-to-date.³⁰⁵

4.7.2. Substance

²⁹⁸ See ICRC Rules (n 35) 9; ICRC Handbook (n 4) 31; IOM (n 1) 81.

²⁹⁹ IOM (n 1) 82.

³⁰⁰ ICRC Handbook (n 4) 92.

³⁰¹ *ibid.*, 31.

³⁰² WFP (n 2) 83; IOM (n 1) 83.

³⁰³ *ibid.*

³⁰⁴ ICRC Handbook (n 4) 144.

³⁰⁵ GDPR (n 49) Article 5(1)(d); ICRC Acquiring and Analysing Data (n 189) 55; ICRC Rules (n 35) Article 9; IOM (n 1) 11; OECD (n 27) 18; WFP (n 2) 16; UN Global Pulse Principles (n 41); USAID (n 44) 8; UNFPA, 'Guidelines on Data Issues in Humanitarian Crisis Situations (UNFPA 2010) <www.unfpa.org/sites/default/files/pub-pdf/guidelines_dataissues.pdf> accessed 22 June 2018, 9; APEC (n 49) 20; OCHA Humanitarianism in the Age of Cyber (n 13) 11; Oxfam (n 39) 2; UNHCR (n 42) 16; ICRC Handbook (n 4) 28; OHCHR (n 38) 17; Commonwealth Model Bill (n 61) 14; ECOWAS (n 49) Article 26; AU Malabo Convention (n 60) Article 13, Principle 4; CoE Convention 108 (n 69) Article 5(4)(d); UN Global Pulse Big Data (n 41) 12; UNDG (n 40) 6.

Data quality requires, *inter alia*, data to be accurate.³⁰⁶ In turn, accuracy refers to the extent to which data reflects reality,³⁰⁷ and to the truthfulness of personal data.³⁰⁸ Data accuracy is necessary (and should be checked) throughout the entire data lifecycle.³⁰⁹ According to the IOM, data controllers should therefore create a “culture of meticulous checking”.³¹⁰

The WFP and ICRC also refer to the need for data to be detailed, ideally first-hand and, where possible, corroborated by different sources.³¹¹ However, collecting first-hand and reliable data is not always possible due to, *inter alia*, high risk environments.³¹² The use of digital technologies through crowdsourcing, for example, could therefore be used as an alternative. However, crowdsourced data can be inaccurate or incomplete as it often contains useless information from secondary sources, and it can therefore be difficult to verify the accuracy of the data.³¹³ When collecting data through crowdsourcing, organizations should attempt to verify it through methods such as triangulation with other credible sources.³¹⁴ Crowdsourced data should be used with discretion³¹⁵ and, when in doubt, marked as unverified.³¹⁶

The Development Policy Research Unit and the ICRC refer to the trade-off between accuracy and timeliness, as collecting reliable data can be a costly and lengthy process.³¹⁷ Timeliness is also mentioned as an important criterion by other organizations.³¹⁸ In addition, some organizations highlight the need for data to be complete³¹⁹ and consistent.³²⁰

Moreover, all reasonable steps should be taken to ensure that data are kept as up-to-date and current as possible,³²¹ to the extent necessary for the purposes of use.³²²

³⁰⁶ ICRC Acquiring and Analysing Data (n 189) 9; IOM (n 1) 11 OECD (n 27) 18; WFP (n 2) 16; UN Global Pulse Principles (n 41); USAID (n 44) 8.

³⁰⁷ Lynn Wolfrey, ‘An Open African Data Approach to Improving Data Quality’ (World Bank Group 2014) 5 <www.dpru.uct.ac.za/sites/default/files/image_tool/images/36/Publications/Policy_Briefs/DPRU%20PB%2014-42.pdf> accessed 22 June 2018, 5; Responsible Data Forum (n 19) 63; APEC, *Privacy Framework* (2005) 20; OCHA Humanitarianism in the Age of Cyber (n 13) 11.

³⁰⁸ IOM (n 1) 36; WFP (n 2) 25.

³⁰⁹ IOM (n 1) 35; ICRC Acquiring and Analysing Data (n 189) 55.

³¹⁰ IOM (n 1) 35.

³¹¹ WFP (n 2) 26; ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence* (2013) 88 (ICRC Professional Standards for Protection).

³¹² ICRC Professional Standards for Protection (n 311) 88.

³¹³ OCHA Building Data Responsibly (n 43) 5.

³¹⁴ ICRC Professional Standards for Protection (n 311) 88.

³¹⁵ OCHA Building Data Responsibly (n 43) 5.

³¹⁶ ICRC Professional Standards for Protection (n 311) 88.

³¹⁷ Lynn Wolfrey (n 307) 5; ICRC Professional Standards for Protection (n 311) 88.

³¹⁸ USAID (n 44) 8; UNFPA 2010 (n 305) 9; Responsible Data Forum (n 19) 52.

³¹⁹ USAID (n 44) 8; APEC (n 49) 20.

³²⁰ ICRC Acquiring and Analysing Data (n 189) 55.

³²¹ IOM (n 1) 11; ICRC Rules (n 35) Article 9; OCHA Humanitarianism in the Age of Cyber (n 13) 11; Oxfam (n 39) 2; WFP (n 2) 16.

³²² APEC (n 49) 20; UNHCR (n 42); OECD (n 27) 18.

Under this principle of data quality, some organizations also refer again to the need for data to be adequate, relevant³²³ (i.e. closely connected or appropriate to the specified purpose),³²⁴ and not excessive in relation to the specified purpose(s).³²⁵ Personal data should therefore be of sufficient quality and quantity to meet those specified purposes.³²⁶

4.7.3. The Principle in Practice

In practice, the accuracy of data could be checked, *inter alia*, by:

- monitoring the collection procedure;
- validating the categories of personal data;
- cross-checking prior to recording and when converting paper records to electronic formats;
- prior checking before use and disclosure; and
- regular reporting and continuous monitoring throughout the lifecycle of data processing.³²⁷

International NGO Medair's experience using a software system to register Syrian refugees in Lebanon has highlighted the need for very frequent spot checks to account for both errors by data collection staff and data subjects providing incorrect data. To facilitate such spot checks, Medair incorporated data triangulation into the process through comparison with refugee registration papers.

328

In order to aid verification of the truthfulness and correctness of the data, where feasible, data subjects should be briefed as to the importance of obtaining accurate data prior to data collection.³²⁹ Furthermore, electronic records should be kept in the most recent formats available, since outdated electronic media can cause corruption of personal data or lead to data loss.³³⁰

Mechanisms should also be put in place to update any data received from a third party should the third party amend their records, and vice versa if the organization updates data received from a third party.³³¹

³²³ OECD (n 27) 18; USAID (n 44) 8; Lynn Wolfrey (n 307) 5; Oxfam (n 39) 2.

³²⁴ WFP (n 2) 25.

³²⁵ IOM (n 1) 35; WFP (n 2) 16; USAID (n 44) 8.

³²⁶ IOM (n 1) 35; WFP (n 2) 25.

³²⁷ IOM (n 1) 36.

³²⁸ Joel Kaiser and Rob Fielding, 'A Principled Approach to Data Management: Lessons Learned from Medair's Experience in Lebanon Using Last Mile Mobile Solutions' in Raquel Llorente and Imogen Wall (eds.) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management* (European Interagency Security Forum 2014) (Joel Kaiser and Rob Fielding) 40.

³²⁹ IOM (n 1) 36.

³³⁰ IOM (n 1) 36.

³³¹ WFP (n 2) 26.

4.8. Transparency and Openness

4.8.1. Definition

Data controllers should provide information about developments, practices and policies regarding the processing personal data.³³²

4.8.2. Substance

Data controllers should conduct their operations following a general policy of transparency and openness towards data subjects and the general public. In some of the frameworks and guidelines considered, transparency is not recognised as a specific principle, but is instead an overarching idea that is present throughout the whole policy;³³³ while in others it is specifically addressed as a separate principle.³³⁴

Transparency relates to the relationship between data controllers and data subjects. Data controllers should have an open line of communication with the very individuals from whom they collect data. Transparency in this regard requires a minimum amount of information to be provided to the data subjects regarding the collection and processing of their personal data. This information usually includes, *inter alia*, whether data is being collected or processed, for what purposes, and by whom. This is addressed in greater detail in chapter 3 under the entitlement to information.

Transparency also includes a degree of disclosure to the general public. Data controllers should ensure that their data policies and practices (for instance how data is collected, how long it is stored, and how privacy is ensured) are transparent and made publicly available.

4.8.3. The Principle in Practice

Regarding data sharing, there may seem to be an initial tension between the disclosing of data encouraged by transparency, and the maintenance of confidentiality of the individual demanded by privacy. Nevertheless, there should be a minimum list of certain data categories that can safely be disclosed without endangering an individual's privacy.³³⁵ Before disseminating data, data controllers should make sure to have

³³² IOM (n 1) Principle 7; OECD (n 27) 15; APEC (n 49) 12-14; ICRC Handbook (n 4) 90-91; ICRC Rules (n 35) Article 2; OHCHR (n 38) 13-14; UNDG (n 40) 7; USAID (n 44) 29; GDPR (n 49) Article 12; OAS Preliminary Principles (n 46) Principle 4; ECOWAS (n 49) Article 27; MSF (n 37) 4-12; WFP (n 2) 20; OCHA Humanitarianism in the Age of Cyber (n 13) 17; AU Malabo Convention (n 60) Article 13(5).

³³³ For example, the UNHCR (n 42) Principle 2.2, states that "The processing may only be carried out [...] in a fair and transparent manner"; and Oxfam (n 39) 4, "encourages data sharing for transparency and accountability purposes".

³³⁴ For example, the ECOWAS data protection act recognises the 'Principle of Transparency' under its Article 27.

³³⁵ Responsible Data Forum (n 19) 64.

implemented all the necessary steps to protect an individual's privacy. They should make a full assessment of privacy risks, in order to identify the information that should not be made public.³³⁶

4.9. Data Security

4.9.1. Definition

Personal data should be protected by reasonable and appropriate physical, technological and organizational measures against unauthorised use, modification, tampering, unlawful destruction, accidental loss, damage and destruction, improper disclosure, or undue transfer.³³⁷

4.9.2. Substance

Data controllers should take 'reasonable' and 'appropriate' measures to secure personal data. These two notions are relative: what constitutes 'reasonable' and 'appropriate' measures may vary depending on the specific context, and therefore requires a form of assessment.

What might constitute 'appropriate' measures to secure personal data depends on a range of factors, listed in Box 17.³³⁸

Box 17: Factors Influencing the Variation of Data Security Measures

- The assessed level of data protection risks
- The nature and sensitivity of the data processed and capacity to cause harm in case of misuse
- The vulnerability of data subjects
- The format of data storage (e.g. electronic or paper records), channel of transfer and their respective vulnerabilities
- The type of activities of the organization
- The context in which the data processing is taking place

Determining the appropriate security measures requires an assessment of the risks inherent in each specific instance of data processing.³³⁹ A number of organizations have included this risk assessment as a part of their

³³⁶ USAID (n 44) 29.

³³⁷ ICRC Handbook (n 4) 31; ICRC Rules (n 35) Articles 16 and 17; IOM (n 1) Principe 8; UN Global Pulse Principles (n 41); UNHCR (n 42) Article 2.8, Parts 4 and 6; USAID (n 44) Section 508.3.9; WFP (n 2) Principle 5; MSF (n 37) 4; UNDG (n 40) Principle 6; OHCHR (n 38) 15; OCHA Humanitarianism in the Age of Cyber (n 13) 11; Oxfam does not refer to data security as a distinct principle, but underlines that the security of data is essential to ensure the right of participants to data activity not to be put at risk, Oxfam (n 39) 4; AU Malabo Convention (n 60); GDPR (n 49) Article 5(1)(f); CoE Convention 108 (n 69) Article 7; Organization of American States (Inter-American Juridical Committee) 'OAS Principles on Privacy and Personal Data Protection' (26 March 2015) CJI/doc. 474/15 rev.2 (OAS Annotated Principles) 11; ECOWAS (n 49) Article 43; APEC (n 49) 21.

³³⁸ Factors enumerated in this Box are mentioned in the following guidelines: WFP (n 2) 90-91; IOM (n 1) 71; UNHCR (n 42) 4.2.1.

³³⁹ On the determination of 'appropriateness', see e.g. the OAS's commentary on data security, OAS Annotated Principles (n 337) Principle 6.

data protection impact assessment (DPIA) procedures.³⁴⁰ DPIAs will be discussed in further detail in the section on the principle of accountability, below.

More sensitive data require a greater level of protection. The guidelines of the IOM offer an example of good practice in that regard. The IOM requires that each data record be systematically and clearly marked after a sensitivity assessment, according to the level of confidentiality required by the sensitivity of the data. This allows the organization to keep track of the level of protection required.³⁴¹

While a risk and security assessment should be conducted at least prior to the collection of data, it should be borne in mind that the threats to data security may change over time, for instance as a result of the apparition of new kinds of cyber threats, deteriorating security situations that pose a threat of personal data breaches,³⁴² or climate hazards.³⁴³ Moreover, insufficiencies in a data security policy might be discovered in practice, for example after the occurrence of a data security breach. This highlights the need to review and upgrade data security measures frequently, which has been underlined in a number of the guidelines studied.³⁴⁴

Some organizations consider that measures should not only be ‘appropriate’, but also ‘reasonable’.³⁴⁵ The reasonable character of a security measure is determined, *inter alia*, in light of the cost and operational feasibility of implementing it, and the availability of technology. Similarly, the UNDG underlines in its guidelines that measures to ensure data security should not disproportionately compromise the utility of the data for the intended purpose.³⁴⁶

4.9.3. The Principle in Practice

The principle of data security requires data controllers to take practical measures to secure data. Box 18³⁴⁷ (below) summarises the organizational, physical and technological security measures developed in practice by organizations committed to mitigating risks to data security.

³⁴⁰ OAS Annotated Principles (n 337) Principle 6; UNHCR (n 42) 4.4.2; WFP (n 2) 85-89; GDPR (n 49) Article 35.

³⁴¹ The categories of confidentiality are the following: ‘unrestricted dissemination’, ‘restricted dissemination’, ‘confidential’ and ‘secret’. The last two categories of confidentiality relate respectively to personal data and highly sensitive personal data, IOM (n 1) 72.

³⁴² For more information on the management of breaches of data security, see principle of accountability below.

³⁴³ OAS Annotated Principles (n 337) 11.

³⁴⁴ OAS Annotated Principles (n 337) Principle 6; APEC (n 49) Principle 7; ICRC Handbook (n 4) 32; IOM (n 1) 71; UNDG (n 40) 6.

³⁴⁵ OECD (n 27) Principle 7; UN Global Pulse Principles (n 41); IOM (n 1) 71; WFP (n 2) 37; OAS Annotated Principles (n 337) Principle 6.

³⁴⁶ UNDG (n 40) 6.

³⁴⁷ The type of security measures included are inspired by the following guidelines: WFP (n 2) 41-43; IOM (n 1) 72-78; UNHCR (n 42) 4.2.4-5; and ICRC Handbook (n 4) 31-35.

Organizational Security Measures	Physical Security Measures	Technological Security Measures Box 18	
<ul style="list-style-type: none"> Establishing and regularly updating a data security policy based on a risk assessment, including for instance physical security guidelines, IT security policy, email security guidelines, guidelines for information classification (i.e. classifying information as public, internal, confidential and strictly confidential), a contingency plan and document destruction guidelines Ensuring that sufficient resources are allocated to enable all security measures to be implemented, for example by including necessary costs in project proposals Training staff and partners handling Personal Data on data security Conducting Data Protection Impact Assessments Granting and updating access to databases containing personal data on a need-to-know basis 	<ul style="list-style-type: none"> Ensuring that paper records and portable electronic devices containing personal data are kept in locked shelves or rooms Restricting access to buildings, offices and shelters to authorised staff Restricting access to storage premises to authorised personnel, for instance by requesting identification cards Ensuring that backup copies of paper records of personal data are routinely made and stored in a separate, secure location that allows for easy transportation in the event of evacuation or relocation Ensuring that paper records of personal data are appropriately destroyed as soon as they are no longer needed. For the destruction of highly sensitive personal data, methods such as shredding or burning can be considered 	Encoding	<ul style="list-style-type: none"> Personal data should be stored in encrypted folders Decryption keys should be safely stored at all times and allocated to designated custodians and ITC officer to avoid operational hazard if keys are lost or misplaced
		Data Coding	<ul style="list-style-type: none"> Identifiers of the data subject should be substituted for codes, in particular when handling categories of highly sensitive personal data or in the absence of encryption tools
		Passwords and Logging-Off	<ul style="list-style-type: none"> Data controllers should ensure that electronic files containing personal data are password-protected Passwords should always be protected, regularly changed and not automatically entered through 'keychain' functions Multiple levels of passwords protection should be used - e.g. one password to log on to a computer and another, different, to access a database Staff handling personal data should check that they have logged off properly from computer systems. Automatic time-out to log off computers can be used
		Back-Ups	<ul style="list-style-type: none"> Effective recovery mechanisms and back-up procedures should cover all electronic records The ITC officer should ensure that backup procedures are done on a regular basis Back-up procedures should be automated to allow for easy recovery, especially in situations where back-up are difficult due to, <i>inter alia</i>, regular power outage or system failure
		Remote Access to Servers	<ul style="list-style-type: none"> 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
		Emails	<ul style="list-style-type: none"> All email correspondence containing personal data, internal and external, should be limited authorised staff on a need-to-know basis. Recipients of email correspondence should be carefully selected to avoid unnecessary dissemination of personal data Emails containing personal data should be highlighted as 'confidential' to identify the sensitivity of the e-mail Emails and attachments containing personal data should be encrypted
		Deletion of Personal Data	<ul style="list-style-type: none"> Electronic records and database no longer needed should be destroyed with the advice of an IT officer to ensure permanent elimination

4.10. Accountability

4.10.1. Definition

Data controllers should be accountable for complying with measures that give effect to the entitlements and principles set out above.³⁴⁸

4.10.2. Substance

The principle of accountability in data processing is premised on the acknowledgment of the responsibility of data controllers to give effect to the entitlements and principles described in chapters 3 and 4 of this report.³⁴⁹ Data controllers should take adequate and proportionate measures to ensure implementation of, and monitor compliance with, these entitlements and principles.³⁵⁰ The adoption of these measures would enable data controllers to demonstrate their compliance with the entitlements and principles, when required.³⁵¹

4.10.3. The Principle in Practice

While many organizations have acknowledged the need for accountability in data processing, in practice, they have developed variable sets of processes to ensure and monitor compliance with the entitlements and principles, tailored to the scale, volume and sensitivity of their data processing.³⁵² By way of a typology, a number of common components of accountability methods of organizations involved in data processing have been identified. Methods to ensure accountability in data processing can be classified into six main categories, discussed below.

³⁴⁸ ICRC Handbook (n 4); ICRC Rules (n 35) Article 15; IOM (n 1) Principle 12; UN Global Pulse Principles (n 41); UNHCR (n 42) Article 2.9 and Chapter 7; OECD (n 27) Principles 14 and 15; USAID (n 44) Article 508.3.5 ff.; APEC (n 49) paragraph 32; WFP (n 2) Principle 4; OAS Annotated Principles (n 337) Principle 10; CoE Convention 108 (n 69) Articles 7 and 10; OCHA Humanitarianism in the Age of Cyber (n 13) 11.

³⁴⁹ ICRC Handbook (n 4) 36.

³⁵⁰ ICRC Handbook (n 4) 36.

³⁵¹ Demonstrating such compliance constitutes an explicit requirement according to the majority of the regulatory frameworks studied and the ICRC Handbook, ICRC Handbook (n 4) 36: GDPR (n 49) Article 5(2); OAS Annotated Principles (n 337) Principle 10; OECD (n 27) Article 15(b); CoE Convention 108 (n 69) Article 10(1).

³⁵² The OECD has, for instance, noted the need for flexibility when putting in place accountability measures: “large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment (...) [Measures to ensure accountability of] data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller’s operations may also impact on the nature of a privacy management programme [i.e. the set of accountability measures], as even a very small data controller may handle extremely sensitive personal data”, OECD (n 27) 24.

4.10.3.1. Data Protection Impact Assessments (DPIAs)

The organizations with the most comprehensive guidelines have deemed data protection impact assessments (DPIAs)³⁵³ to be a key component of accountability.³⁵⁴ DPIAs have been described as a “tool and process for assessing the protection impact on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimise such impact.”³⁵⁵ DPIAs are required when designing a project, policy, programme or other initiative requiring the processing of personal data, and should be reviewed when the situation changes, or as new risks arise.³⁵⁶

Risks identified by a DPIA may sometimes be so high that the anticipated benefits of the data processing do not significantly outweigh these risks. This could, for instance, be the case when no satisfactory measures have been identified to mitigate such risks.³⁵⁷ In other instances, a DPIA may be unable to assess the potential risks linked with data processing, and thus unable to identify measures to mitigate these risks.³⁵⁸ In such cases, the IOM and OCHA consider that data processing activities should be ceased immediately.³⁵⁹

4.10.3.2. Training

The training of all staff members handling data (at all stages of the data lifecycle) is an important tool to introduce a ‘culture of data protection’ in organizations processing data.³⁶⁰ Such training ensures that the relevant staff members are fully aware of the guidelines governing data processing, the measures to be taken to comply with them, as well as the potential security risks and the procedures to report incidents and mitigate potential harms.³⁶¹

³⁵³ Sometimes also referred to as 'Privacy Impact Assessment' or 'Risk-benefit assessment', WFP (n 2) 15; IOM (n 1) 16.

³⁵⁴ ICRC Handbook (n 4) 36, 63-67; ICRC Rules (n 35) Article 17; WFP (n 2) 15-16, 85-91; UNHCR (n 42) Article 4(5); IOM (n 1) 16-17; OCHA Building Data Responsibility (n 43) 12. Conducting a 'risk assessment' or 'privacy risk assessment' is recommended by the OAS Annotated Principles (n 337) Principle 10; OECD (n 27) Article 15. Under the GDPR, conducting a DPIA constitutes an obligation for data controllers in certain circumstances, GDPR (n 49) Article 35.

³⁵⁵ UNHCR (n 42) 10.

³⁵⁶ A step-by-step guide for organizations on how to conduct a DPIA can be found, *inter alia*, in ICRC Handbook (n 4) 64-67, as well as in WFP (n 2) 85-91.

³⁵⁷ IOM (n 1) 16.

³⁵⁸ OCHA Building Data Responsibility (n 43) 10.

³⁵⁹ OCHA Building Data Responsibility (n 43) 10; IOM (n 1) 16.

³⁶⁰ See e.g. IOM (n 1) 97; ICRC Handbook (n 4) 36; OCHA Building Data Responsibility (n 43) 18; UNHCR (n 42); WFP (n 2) Article 4.2.4(ii); Al Lutz and others, 'Data Protection, Privacy and Security for Humanitarian & Development Programs' (Sherrie Simms ed, World Vision 2017) <www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20&%20Security%20for%20Humanitarian%20%20&%20Development%20Programs%20-%20FINAL.pdf> accessed 22 June 2018 (Al Lutz and others) 6; USAID (n 44) Section 508.3.5.8 (which provides that USAID employees must complete a training every year). The guidelines of some organizations expressly exclude staff members lacking appropriate training and experience from the processing of sensitive information, especially when collected from vulnerable groups, see e.g. WFP (n 1) 108; Oxfam (n 39) 4; and OHCHR (n 38) 12. Some regional organizations recommend data controllers to ensure that employees who handle personal data are appropriately trained, see e.g. OECD (n 27) 16; OAS Annotated Principles (n 337) 16; GDPR (n 49) Article 39(1)(b).

³⁶¹ Al Lutz and others (n 362) 8.

4.10.3.3. Oversight Mechanisms

Data controllers should establish mechanisms to monitor compliance with their data protection guidelines.³⁶² Such monitoring can be conducted by an external or internal auditing body and/or by appointed staff members, usually referred to as Data Protection Officers (DPOs). Box 19 lists some of the most common responsibilities of DPOs.³⁶³

Box 19: Responsibilities of DPOs

- Providing advice, support and training on data protection
- Monitoring and reporting on the implementation of the guidelines
- Documenting data processing activities, including any DPIAs carried out, data transfer agreements, data breach notifications, and complaints by data subjects
- Receiving complaints of data subjects and/or allegations of non-compliance with data protection guidelines
- Identifying effective responses to data protection breaches
- Undertaking investigations into cases of misconduct
- Ensuring that data protection guidelines are regularly reviewed

In addition to the appointment of a DPO, some organizations have deemed it necessary to designate data protection ‘focal points’ in each of the regions or countries where they operate.³⁶⁴ This ensures that the dissemination, training and monitoring regarding the relevant guidelines are not limited to the headquarters.

A recent audit of the data processing activities of the WFP illustrates how internal reviews and the appointment of staff in charge of data protection can contribute to the effective implementation of data protection policies. Although the auditing body considered that the WFP had well-defined data protection and privacy policies, the audit uncovered numerous serious cases of non-compliance that could compromise the safety of data subjects. One of the underlying causes highlighted was the insufficient resources allocated to the effective implementation of the data protection policy in the field, with only two employees supporting the implementation of the policy in 85 country offices and 6 regional bureaux. Following these findings, the WFP committed to implementing the recommendations of the audit.

365

³⁶² ICRC Rules (n 35) Article 26; IOM (n 1) 97; Oxfam (n 39) 5; UNHCR (n 42) 4; WFP (n 2) 10.

³⁶³ This list is based on the guidelines of the following organizations: IOM (n 1) 97; ICRC Rules (n 35) Article 26; WFP (n 2) 10; UNHCR (n 42) Article 7.3.

³⁶⁴ IOM (n 1) 97; UNHCR (n 42) Articles 7.1, 7.2.1; WFP (n 2) 10.

³⁶⁵ WFP Office of the Inspector General, ‘Internal Audit of Beneficiary Management: Internal Audit Report AR/17/17’ (WFP 2017) <<https://docs.wfp.org/api/documents/WFP-0000040084/download/>> accessed 21 June 2018); Ben Parker, ‘Audit exposes UN food agency’s poor data-handling’ *IRIN News* (Geneva, 18 January 2018) <www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling> accessed 21 June 2018.

4.10.3.4. Responses in Cases of Data Breach and (Allegations of) Non-Compliance with a Responsible Data Policy

Data controllers should effectively respond to data breaches (i.e. incidents “leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.”)³⁶⁶ Upon discovery, the staff member(s) in charge of responding to such a breach should be immediately notified.³⁶⁷ Risks associated with the breach should then be assessed.³⁶⁸ When the breach would put data subjects at risk, data controllers should inform those concerned of the breach without undue delay.³⁶⁹ Adequate mitigation measures should be taken to contain the breach where possible, and to mitigate the harm or risk of harm resulting for the data subject(s).³⁷⁰

Similarly, allegations of non-compliance with their responsible data processing policies should be reported by staff members to the individual or body in charge of monitoring the implementation of the guidelines.³⁷¹ Such complaints should then be investigated without undue delay.³⁷² If a complaint is found to be justified, adequate measures should be taken to mitigate the harm or risk of harm resulting for the data subject(s) concerned.³⁷³ Improvement of policies and practices should also be considered to prevent repeated instances of non-compliance.³⁷⁴ The guidelines of some organizations stipulate that staff members involved in cases of non-compliance, which result in a serious breach of, or harm to, the interests or rights of a data subject, may be subject to disciplinary measures.³⁷⁵

4.10.3.5. Internal Means of Remediation

Some organizations underline the need to set up mechanisms by which a data subject can address complaints when their interests or entitlements have been adversely affected by a failure to comply with responsible data guidelines.³⁷⁶ Data subjects should be informed at the moment of the data collection about how and where they can address complaints regarding the handling of their data.³⁷⁷

³⁶⁶ UNHCR (n 42) 11.

³⁶⁷ WFP (n 2) 34; UNHCR (n 42) 4.4.

³⁶⁸ WFP (n 2) 35.

³⁶⁹ ICRC Rules (n 35) Article 20; OECD (n 27) Principles 14 and 15; UNHCR (n 42) Article 4.4.2; GDPR (n 49) Recital 86; WFP (n 2) 35; USAID (n 44) 508.3.9.4.

³⁷⁰ WFP (n 2) 35.

³⁷¹ See e.g. ICRC Rules (n 35) Article 25(4); IOM (n 1) 99.

³⁷² ICRC Rules (n 35) Article 25(4); IOM (n 1) 99.

³⁷³ ICRC Rules (n 35) Article 25(4); IOM (n 1) 99; WFP (n 2) 35; APEC (n 49) 33; OECD (n 27) Principle 15(a)(v).

³⁷⁴ IOM (n 1) 99; WFP (n 2) 33.

³⁷⁵ IOM (n 1) 99; ICRC Rules (n 35) Article 25(5); WFP (n 2) 35;; USAID (n 44) Section 508.3.3.1-2.

³⁷⁶ See, e.g. ICRC Rules (n 35) Article 13; IOM (n 1) 99; UNHCR (n 42) Article 7.3.1 (ii).

³⁷⁷ ICRC Rules (n 35) Article 7(1)(e); WFP (n 2) 35; OECD (n 27) 16, 26; UNHCR (n 42) Article 3(1)(viii).

When reviewing a project involving primary data collection in Lebanon, NGO Medair found that data subjects were not specifically informed that they were entitled to follow up on the use of their data via a hotline for beneficiary complaints. Subsequently, such information was added to the programme leaflet.

378

4.10.3.6. Accountability Measures for Data Sharing

Data controllers continue to be accountable to data subjects when their data are shared.³⁷⁹ Data controllers must therefore be “able to demonstrate that adequate and proportionate measures have been undertaken to ensure compliance with basic data protection principles” by the recipient.³⁸⁰ To this effect, good practices include conducting a DPIA relating to the transfer,³⁸¹ defining the responsibilities of all parties processing the data in a binding instrument (often referred to as data sharing agreement), such as by way of a contract,³⁸² as well as keeping internal records of the transfer.³⁸³

4.11. Concluding Remarks

The data protection principles identified for the purposes of this report, namely legitimate processing, informed consent, purpose limitation, data minimisation, storage limitation, data quality, transparency and openness, data security, and accountability, have each been defined, followed by an explanation of the substance of the principle and guidance for its implementation in practice.

As has been seen, many of the data protection principles discussed in this chapter directly relate to the entitlements of data subjects identified in chapter 3, in that they advocate for the establishment of procedures to allow for the exercise of these entitlements. In certain circumstances, the application of a data protection principle can also limit an entitlement of a data subject, since they are not always absolute. Moreover, the data protection principles themselves inevitably interact with one another, and must therefore be considered together as a whole, in terms of a responsible approach to data, rather than individually in a vacuum.

³⁷⁸ Joel Kaiser and Rob Fielding (n 328) 41.

³⁷⁹ ICRC Handbook (n 4) 60; APEC (n 49) Principle 26; OAS Annotated Principles (n 337) Principle 10; OECD (n 27) 16.

³⁸⁰ This is reflected in ICRC Rules (n 35) Article 15(2). See also e.g. APEC (n 49) Principle 26; OECD (n 27) Principle 26; WFP (n 2) 33.

³⁸¹ ICRC Handbook (n 4) 60.

³⁸² ICRC Rules (n 35) Article 15(2); OECD (n 27) 23; UNHCR (n 42) Articles 6.2 and 7.2.2 (v).

³⁸³ ICRC Handbook (n 4) 60; ICRC Rules (n 35) Article 15(2).

5. CONCLUSIONS

5.1. Observations: Remaining Challenges

The development of a responsible approach to data remains a work in progress. Over the course of this research, a number of challenges, left unresolved by the frameworks and guidelines studied, have become apparent. This final chapter highlights some of these challenges, so that they may be borne in mind if inspiration is to be drawn from this report. In particular, this report has identified two major challenges: the risks emanating from demographically or community identifiable information; and the practical implementation of the entitlements of data subjects.

5.1.1. Risks Emanating from Demographically or Community Identifiable Information

The scope of the majority of the frameworks and guidelines studied is limited to personal data, i.e. “any information relating to an identified or identifiable natural person”,³⁸⁴ which includes personally identifiable information (PII). Yet, some concerns have been raised about the harm that ‘demographically’ or ‘community identifiable information’ (DII or CII) can cause.³⁸⁵ DII or CII have been described as “either individual and/or aggregated data that allow inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age health, condition, location, occupation, and/or other demographically defining factors”.³⁸⁶ These concerns stem from the fact that some threats are collective, i.e. related to groups rather than individuals.³⁸⁷ For example, groups may be discriminated against, or targeted, in situations such as armed conflict or other instances of violence.

This can be illustrated by way of a hypothetical example. An NGO relies on high-resolution satellite imagery to observe a region involved in an armed conflict fuelled by ethnic tensions, to detect threats to the civilian population, and collect images that could constitute (corroborating) evidence of mass atrocities. The NGO releases a report mentioning the fact that civilians (of a certain ethnicity) have had to flee the violence. They support this assertion by providing a related recent satellite image, depicting a camp of internally displaced people. These data are not PII, as no persons can be individually identified from the satellite imagery. However, the data could enable a party to the armed conflict to estimate the number of people in that camp by counting the number of tents, and locate it by comparing the satellite image with existing maps. This could constitute information enabling this party to the armed conflict to locate and attack the group.

³⁸⁴ ICRC Handbook (n 4) 9.

³⁸⁵ See e.g. Linnet Taylor (n 48); Nathaniel Raymond (n 48).

³⁸⁶ Nathaniel Raymond (n 48) 93.

³⁸⁷ ICRC Handbook (n 4) 17.

The little attention devoted to the threats posed by the processing of DII or CII are considered to be a blind spot of the current data protection frameworks and guidelines.³⁸⁸ In order to fill this gap, two issues should be addressed. Firstly, a responsible approach to DII or CII requires an understanding of the fact that it poses risks, as well as an understanding of what these specific risks actually are. Secondly, a responsible approach to DII or CII requires the development of measures to mitigate the risks identified. However, directly converting guidelines which are tailored specifically towards the responsible processing of *personal data* to guidelines for the purpose of responsibly processing *DII or CII* might not always be possible or, indeed, sufficient. For instance, consent and privacy have been conceptualised as relating to individuals. Questions thus remain concerning, for example, what could constitute group privacy, how it could be protected,³⁸⁹ whether groups would need to consent to data processing about them, and how that could be achieved.³⁹⁰

5.1.2. The Practical Implementation of Entitlements of Data Subjects

A second challenge lies in the practical implementation of the entitlements of data subjects. The importance of the entitlements is recognised by many of the frameworks and guidelines studied, and a number of organizations have underlined the need to set up mechanisms to exercise these entitlements. However, even the most detailed guidelines do not explain what forms those mechanisms could take.³⁹¹ This lack of practical guidance could be attributed to the fact that data controllers have not felt the need to provide such a level of detail regarding their implementation mechanisms. However, this could also be due to the fact that they do not actually have any mechanisms in place, which would render the entitlements purely theoretical.

Implementing these entitlements can be very challenging, especially regarding access, correction, erasure and objection, as they cannot be fulfilled collectively (for example, by providing information collectively to a group). Rather, they require individual action (for example, by providing individual access to a data subject requesting such access). In the scenario where a considerable number of data subjects wish to exercise their entitlements, implementation could become an overwhelming task.

³⁸⁸ Nathaniel Raymond (n 48) 84.

³⁸⁹ Lanah Kammourieh and others, 'Group Privacy in the Age of Big Data' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017) 57.

³⁹⁰ *ibid*, 39.

³⁹¹ With the exception of the WFP, see below.

For example, an NGO processing personal data about a group of people has in place a responsible data policy. When collecting the data they explain to the data subjects that they have an entitlement to access, correction, erasure and objection. However, if four hundred illiterate citizens were to request to access or correct their personal data, the NGO might feel it lacks the necessary resources, or might not have mechanisms in place, that would allow it to implement those requests in practice. This lack of mechanisms by which to implement the entitlements of data subjects hinders a responsible approach to data, leaving data subjects unable to meaningfully exercise their entitlements.

In light of these challenges, solid and efficient mechanisms are required to give full effect to the entitlements of data subjects. The WFP has suggested mechanisms that could be established to allow data subjects to request information about their personal data, as well as to correct, update, or erase this data. These mechanisms include the following:

- Providing beneficiaries with contact details of the organization's local offices and the member of staff responsible for the implementation and monitoring of data protection (addresses, telephone numbers and email addresses); and
- Relying on existing mechanisms that enable beneficiaries to give feedback and lodge complaints about the organization's programme in general, such as feedback desks at the project site, complaint boxes or hotlines.³⁹²

Although this is a step in the right direction, additional mechanisms, specifically geared towards giving effect to the entitlements of data subjects, might still be necessary to fully address the challenges highlighted above.

5.1.3. The Way Forward: Transparency as Part of the Solution?

The guidance provided in this report illustrates the value that can be gained from relying on an analysis of a compilation of policies and practice of a range of actors processing data. In the same vein, a constructive debate between those same actors could form an essential part of the solution to tackle the challenges outlined above, namely mitigating the risks involved with DII or CII, and developing more practical measures for the implementation of the entitlements of data subjects.

Instances when data processing goes wrong (for example, a data breach) can have serious consequences, not only for the data subject, but also for the data controller. The general public is seldom made aware of these instances because they are rarely published by the data controllers in question. Yet, sharing details of

³⁹² WFP (n 2) 32.

these incidents would prove to be an invaluable learning experience, not only for the entity evaluating their project, but also for other data controllers seeking to process data responsibly.

This is evidenced by a notable exception to the rare instances of publication of when data processing goes wrong.³⁹³ Harvard Humanitarian Initiative (HHI) (involved in the project from 2010 to 2012) has reported³⁹⁴ on the struggles experienced in processing data responsibly in the context of the Satellite Sentinel Project (SSP). This project operated until 2015 in the border region of Sudan and South Sudan, attempting to detect threats to the civilian population through the analysis of high-resolution satellite imagery.³⁹⁵ Interestingly, the risks identified concerned the handling and disclosure of demographically identifiable information (DII), a challenge identified above. The publication of the risks and harms involved in the SSP is an important step, since this allows other actors to take steps to mitigate the same risks and protect against the same harms in the future. Furthermore, this prompted the launch, by HHI, of the Signal Program on Human Security and Technology in 2012, to address the ethical challenges identified in relation to the SSP. The Signal Program has subsequently produced the Signal Code,³⁹⁶ a document taking a human rights approach to information during crisis situations, which is an important contribution to this field.

To be truly constructive, therefore, the continuation of the discussion of a responsible approach to data must be as transparent as possible. As has been highlighted, it is important that instances where data subjects have been harmed and/or instances where organizations have experienced challenges and difficulties are discussed openly.

5.2. Final Remarks

Humanitarian, human rights and development organizations can only fully harness the opportunities offered by data if they adopt a responsible approach thereof, one that mitigates risks of harm inherent in data processing. Yet, there is an observable difficulty in implementing a responsible approach to data, particularly because of the lack of awareness of what such a responsible approach entails and, more importantly, how it can be implemented in practice.

³⁹³ The WFP also opted for a transparent approach by publicising audits conducted on compliance with their internal data protection policy. ³⁹³ WFP Office of the Inspector General, 'Internal Audit of Beneficiary Management: Internal Audit Report AR/17/17' (WFP 2017) <<https://docs.wfp.org/api/documents/WFP-0000040084/download/>> accessed 21 June 2018).

³⁹⁴ See e.g. Nathaniel Raymond and others, 'While We Watched: Assessing the Impact of the Satellite Sentinel Project' (2013) 14(2) *Georgetown Journal of International Affairs* 185.

³⁹⁵ OCHA Building Data Responsibility (n 43) 10.

³⁹⁶ The Signal Code (n 115).








Against this backdrop, the present report aimed to provide guidance for organizations working with data and seeking to process data in a responsible manner, or to help them to improve their pre-existing policies. To this end, this report relied on a comparative analysis of the existing regional and international data protection frameworks, as well as guidelines developed by humanitarian, human rights and development organizations.

This comparative analysis enabled the report to identify the core components of a responsible approach to data. These core components were divided into two categories, namely entitlements of data subjects (an entirely new means by which to classify these types of component, coined for purposes of this report and discussed in chapter 3.1.), and data protection principles. The entitlements of data subjects to privacy, information, access, correction, erasure, objection and participation were discussed in chapter 3, while the data protection principles, relating to legitimate processing, informed consent, purpose limitation, data minimisation, storage limitation, data quality, transparency and openness, data security, and accountability were discussed in chapter 4. The comparative analysis was relied upon to explain the scope and content of each of these core components, and to provide guidance as to how to implement them in practice.

When brought together, the frameworks and guidelines studied in this report offer an invaluable set of considerations, as well as practical measures and mechanisms, to responsibly process data. This combination constitutes solid guidance for organizations working with data and seeking to process it in a responsible manner.

Yet, the development of a responsible approach to data remains a work in progress. Eventually, and ideally, efforts in this regard might lead towards the emergence of a less fragmented and more comprehensive data protection regulatory landscape (discussed in chapter 2), as well as the tackling of certain remaining challenges to data protection (such as the mitigation of risks emanating from DII or CII and the development of practical measures to give effect to the entitlements of the data subjects, discussed above). While this report provides a comprehensive overview of the current state of the art, it does not claim to constitute *the* definitive guide in responsible data processing. Instead, this report offers a number of considerations that are a step in the right direction towards a responsible approach to data.

Annex 1: Entitlements of Data Subjects

	Privacy	<i>Data subjects should have control over who can access and manage their personal data. Unless consented thereto, data disclosed to data collectors should be protected and kept private.</i>
	Information	<i>Data subjects are entitled to be made aware of the fact that they are participating in data processing.</i>
	Access	<i>Data subjects are entitled to access to their own personal data.</i>
	Correction	<i>Data subjects are entitled to request that a data controller rectifies any mistakes or inaccuracies in the personal data relating to them.</i>
	Erasure	<i>Data subjects are entitled to have their personal data deleted if the continued processing of those data is not justified.</i>
	Objection	<i>Data subjects are entitled to object, on grounds relating their specific situation, to the processing of their personal data.</i>
	Participation	<i>Relevant population groups are entitled to be involved in data processing exercises, including planning, data collection, dissemination and analysis of data.</i>

Annex 2: Data Protection Principles



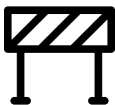






	Legitimate Processing	<i>Personal data should only be processed on a legitimate basis.</i>
	Informed Consent	<i>Data subjects should agree to the processing of their personal data by providing consent, which must be obtained voluntarily and with full knowledge of all the relevant implications.</i>
	Purpose Limitation	<i>Personal data should be collected for specified, explicit and legitimate purposes and should not be further processed in a manner that is incompatible with those purposes.</i>
	Data Minimisation	<i>Personal data should be adequate, relevant and not excessive in relation to the specified purpose(s).</i>
	Storage Limitation	<i>Personal data should only be retained for as long as is necessary to achieve the specified purpose(s).</i>
	Data Quality	<i>Personal data should be accurate, complete and kept up-to-date.</i>
	Transparency and Openness	<i>Data controllers should provide information about developments, practices and policies regarding the processing of personal data.</i>
	Data Security	<i>Personal data should be protected by reasonable and appropriate physical, technological and organizational measures against unauthorised use, modification, tampering, unlawful destruction, accidental loss, damage and destruction, improper disclosure or undue transfer.</i>
	Accountability	<i>Data controllers should be accountable for complying with measures that give effect to the entitlements and principles stated above.</i>

Table of Cases

Amann v Switzerland (2000) no. 27798/95 ECHR 2000-II.

United States v Microsoft Corporation, 584 US Supreme Court (2018)

Table of International Legislation

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (opened for signature 28 January 1981, entered into force 1 October 1985) ETS 108 (CoE Convention 108)

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3

International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990, entered into force 1 July 2003) 2220 UNTS 3

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

Council of the OECD, 'Revised Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (11 July 2013) (OECD)

Protocol to the Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, regarding supervisory authorities and transborder data flows (opened for signature 8 November 2001 entered into force 1 July 2004) ETS 181 (Protocol to CoE Convention 108)

UNHRC 'General Comment 16' in 'Article 17, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (adopted 8 April 1988) HRI/GEN/1/Rev.9 (Vol. I)

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR)

Table of Regional Legislation

African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) (AU Malabo Convention)

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) OAS Treaty Series No 36

Charter of Fundamental Rights of the European Union (adopted 12 December 2007, entered into force 1 December 2009) OJ 2010 C 83/389

European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1990) ETS 5, 213 UNTS 221

Supplementary Act on Personal Data Protection within ECOWAS (adopted 16 February 2010) (ECOWAS)

Table of Resolutions of Regional Organizations and Documents of Regional Bodies

African Union (Commission of the African Union and Internet Society) 'Personal Data Protection Guidelines for Africa' (9 May 2018) (AU Guidelines)

Asia-Pacific Economic Cooperation (Secretariat) 'Privacy Framework' (2005) APEC#205-SO-01.2 (APEC)

Commonwealth (Commonwealth Law Ministries and Secretariat) 'Model Bill on the Protection of Personal Information' (approved by the Commonwealth Law Ministries 17 October 2005, published by the Secretariat 2017) (Commonwealth Model Bill)

Organization of American States (Committee on Juridical and Political Affairs of the Permanent Council of the Organization of American States) 'Preliminary Principles and Recommendations on Data Protection' (17 October 2011) CP/CAJP-2921/10 (OAS Preliminary Principles)

Organization of American States (Inter-American Juridical Committee) 'OAS Principles on Privacy and Personal Data Protection' (26 March 2015) CJI/doc. 474/15 rev.2 (OAS Annotated Principles)

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 (2016) OJ 2016 L 119/1 (GDPR)

Guidelines of Humanitarian, Human Rights and Development Organizations Studied

Al Achkar Z, and others, 'Building Data Responsibility into Humanitarian Action' (Lilian Barajas and Matthew Easton eds, OCHA Policy and Studies Series, OCHA 2016)

<www.unocha.org/sites/unocha/files/Building%20data%20responsibility%20into%20humanitarian%20action.pdf> accessed 22 June 2018

Gilman D, 'Humanitarianism in the Age of Cyber-Warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies' (Matthew Easton ed, OCHA Policy and Studies Series, OCHA 2014) <www.unocha.org/sites/unocha/files/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%202011.pdf> accessed 22 June 2018

ICRC, 'ICRC Rules on Personal Data Protection' (ICRC 2016) <https://shop.icrc.org/icrc-rules-on-personal-data-protection.html?store=default&from_store=fr> accessed 21 June 2018

IOM, 'IOM Data Protection Manual' (IOM 2010)

<https://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf> accessed 9 June 2018

Kuner C, and Marelli M, (eds), *Handbook on Data Protection in Humanitarian Action* (International Committee of the Red Cross 2017) <<https://shop.icrc.org/icrc/pdf/view/id/2592>> accessed 21 June 2018

MSF, 'MSF Data Sharing Policy' (MSF 2013)

<<http://fieldresearch.msf.org/msf/bitstream/10144/306501/1/MSF+data+sharing+policy+final+061213.pdf>> accessed 21 June 2018

OHCHR, 'A Human Rights-based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development' (OHCHR 2015)

<www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf> accessed 9 June 2018

Oxfam, 'Responsible Program Data Policy' (Oxfam 2015)

<www.oxfam.org/sites/www.oxfam.org/files/file_attachments/story/oxfam-responsible-program-data-policy-feb-2015-en.pdf> accessed 21 June 2018

UN Global Pulse, 'Big Data for Development and Humanitarian Action Towards Responsible Governance' (UN Global Pulse 2016)

<http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_0.pdf> accessed 21 June 2018

UNDG, 'Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda' (UNDG 2017) <https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf> accessed 21 June 2018

UNHCR, 'Policy on the Protection of Personal Data of Persons of Concern to UNHCR' (UNHCR 2015)

<www.refworld.org/docid/55643c1d4.html> accessed 9 June 2018

USAID, 'ADS Chapter 508: Privacy Program' (USAID 2014)

<www.usaid.gov/sites/default/files/documents/1868/508.pdf> accessed 21 June 2018

WFP, 'WFP Guide to Personal Data Protection and Privacy' (WFP 2016)

<<https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/>> accessed 9 June 2018

Bibliography

Books

ACAPS, *Humanitarian Needs Assessment: The Good Enough Guide* (Emergency Capacity Building Project and Practical Action Publishing 2014)

Barker RL, *The Social Work Dictionary* (National Association of Social Work 1995)

Chalmers D, Davis G, and Monti G, *European Union Law* (Cambridge University Press 2014)

Clark K, and others, *Guidelines for the Ethical Use of Digital Data in Human Research* (The University of Melbourne and Carlton Connect Initiative 2015)

Fujita S, *The World Bank, Asian Development Bank and Human Rights: Developing Standards of Transparency, Participation and Accountability* (Edward Elgar Publishing 2013)

Neef D, *Digital Exhaust: What Everyone Should Know about Big Data, Digitization and Digitally Driven Innovation* (Pearson Education 2014)

Richardson G, (ed), *Social Media and Politics: A New Way to Participate in the Political Process* (ABC-CLIO 2016)

Rothman J, *Practice with Highly Vulnerable Clients* (Prentice-Hall 1994)

Schenk K, and Williamson J, *Ethical Approaches to Gathering Information from Children and Adolescents in International Settings: Guidelines and Resources* (Population Council 2005)

<www.popcouncil.org/uploads/pdfs/horizons/childrenethics.pdf> accessed 21 June 2018

Book Articles

Forgó N, Hanöld S, and Schutze B, 'The Principle of Purpose Limitation and Big Data' in Corrales M, Fenwick M, and Forgó N, (eds), *New Technology, Big Data and the Law* (Springer 2017)

Kaiser J, and Fielding R, 'A Principled Approach to Data Management: Lessons Learned from Medair's Experience in Lebanon Using Last Mile Mobile Solutions' in Llorente R, and Wall I, (eds) *Communications technology and humanitarian delivery: challenges and opportunities for security risk management* (European Interagency Security Forum 2014)

Kammourieh L, and others, 'Group Privacy in the Age of Big Data' in Taylor L, Floridi L and van der Sloot B, (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

Meier P, 'Big (Crisis) Data: Humanitarian Fact-Finding with Advanced Computing' in Alston P, and Knuckey S (eds), *The Transformation of Human Rights Fact-Finding* (Oxford University Press 2016)

Raymond N, 'Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data' in Taylor L, Floridi L and van der Sloot B, (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

Taylor L, 'Group Privacy and Data Ethics in the Developing World' in Taylor L, Floridi L and van der Sloot B, (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017)

Journal Articles

Angucia M, Zeelen J, and de Jong G, 'Researching the Reintegration of Formerly Abducted Children in Northern Uganda through Action Research: Experiences and Reflections' (2010) 20 *Journal of Community and Applied Social Psychology* 217

Burfoot D, 'Children and young people's participation, Arguing for a better future' (2003) 3 *Youth Studies Australia* 44

Clacherty G, and Donald D, 'Child participation in research: Reflections on ethical challenges in the southern African context' (2007) 6 *African Journal of AIDS Research* 147

Ellard-Gray A, and others, 'Finding the Hidden Participant: Solutions for Recruiting Hidden, Hard-to-Reach, and Vulnerable Populations' (2015) 10 *International Journal of Qualitative Methods* 1

Fonjong L, 'Fostering Women's Participation in Development through Non-Governmental Efforts in Cameroon' (2001) 3 *The Geographical Journal* 223

Freeman L, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials' (2018) 41 *Fordham International Law Journal* 283

Raymond N, and others, 'While We Watched: Assessing the Impact of the Satellite Sentinel Project' (2013) 14(2) *Georgetown Journal of International Affairs* 185.

Tabbush C, 'The elephant in the room: silencing everyday violence in rights-based approaches to women's community participation in Argentina' (2010) 3 Community Development Journal 325

Wang B, and others, 'Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities' (2013) 2 Stability: International Journal of Security and Development 1

Young L, and Barrett H, 'Ethics and participation: Reflections on research with street children' (2001) 4 Ethics, Place & Environment 130

Online Journals

Hoogeveen JG, and others, 'A Guide to the Analysis of Risk, Vulnerability and Vulnerable Groups' (2004) Researchgate

<www.researchgate.net/publication/238528462_A_Guide_to_the_Analysis_of_Risk_Vulnerability_and_Vulnerable_Groups> accessed 21 June 2018

Conference Papers

-- 'International Standards on the Protection of Personal Data and Privacy' (International Conference of Data Protection and Privacy Commissioners, 5 November 2009)

<https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_en.pdf> accessed 22 June 2018

-- 'Resolution on the urgent need for protection privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection' (International Conference on Data Protection and Privacy Commissioners, Strasbourg, 17 October 2008)

<<https://icdppc.org/wp-content/uploads/2015/02/Resoluion-on-the-urgent-need-for-protecting-privacy-in-a-borderless-world.pdf>> accessed 22 June 2018.

Baar T, Deligianni A, and Stettina CJ, 'Data-Driven Innovation for NGO's: How to define and mobilise the Data Revolution for Sustainable Development?' (Data Policy Conference, Cambridge, September 2016)

<www.researchgate.net/publication/311002010> accessed 16 June 2018

Publications of Organizations (other than those studied)

Berman G, and others, 'What We Know About Ethical Research Involving Children in Humanitarian Settings: An overview of principles, the literature and case studies' (Innocenti Working Paper, UNICEF 2016) <www.unicef-irc.org/publications/849-what-we-know-about-ethical-research-involving-children-in-humanitarian-settings-an.html> accessed 21 June 2018

European Union (European Commission) 'Communication from the Commission to the European Parliament and the Council on Stronger Protection, New Opportunities: Commission guidance on the direct application of the application of the General Data Protection Regulation as of 25 May 2018 (2018

Global Initiative for Economic, Social and Cultural Rights, 'A GI-ESCR Practitioner's Guide' (Global Initiative for Economic, Social and Cultural Rights 2014) <<http://globalinitiative-esqr.org/wp->

<content/uploads/2014/05/GI-ESCR-Practitioners-Guide-on-Right-to-Participation.pdf>> accessed 21 June 2018

Greenwood F and others, 'The Signal Code. A Human Rights Approach to Information During Crisis' (Harvard Humanitarian Initiative 2017)

<http://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf> accessed 22 June 2018

ICRC, 'Acquiring and Analysing Data in Support of Evidence-based Decisions: A Guide for Humanitarian Work' (ICRC 2017) <www.icrc.org/en/publication/acquiring-and-analysing-data-support-evidence-based-decisions-guide-humanitarian-work> accessed 21 June 2018

ICRC, 'Professional Standards for Protection Work: Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence' (ICRC 2013)

IFRC, 'Community early warning systems: guiding principles' (IFRC 2012)

<www.ifrc.org/PageFiles/103323/1227800-IFRC-CEWS-Guiding-Principles-EN.pdf> accessed 21 June 2018

Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (Information Commissioner's Office 2018) <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>> accessed 22 June 2018

Lutz A, and others, 'Data Protection, Privacy and Security for Humanitarian & Development Programs' (Simms S, ed, World Vision 2017) <www.wvi.org/sites/default/files/Discussion%20Paper%20-%20Data%20Protection%20Privacy%20&%20Security%20for%20Humanitarian%20%20&%20Development%20Programs%20-%20FINAL.pdf> accessed 22 June 2018

Lynn Wolfrey, 'An Open African Data Approach to Improving Data Quality' (World Bank Group 2014) <www.dpru.uct.ac.za/sites/default/files/image_tool/images/36/Publications/Policy_Briefs/DPRU%20PB%2014-42.pdf> accessed 22 June 2018

Okeleke K, 'Refugees and Identity: Considerations for Mobile-Enabled Registration and Aid Delivery' (GSMA 2017) <www.gsmaintelligence.com/research/2017/09/refugees-and-identity-considerations-for-mobile-enabled-registration-and-aid-delivery/644/> accessed 21 June 2018

Responsible Data Forum, 'The Handbook of the Modern Development Specialist: Being a Complete Illustrated Guide to Responsible Data Usage, Manners & General Deportment' (The Engine Room Responsible Data Program 2016) <<https://responsibledata.io/2016/04/13/the-release-of-the-hand-book-of-the-modern-development-specialist/>> accessed 21 June 2018

The Engine Room, Benetech and Amnesty International, 'Datnav: How to navigate digital data for human rights research' (2016) <www.theengineroom.org/wp-content/uploads/2016/09/datnav.pdf> accessed 16 June 2018

The Engine Room, *Responsible Data at Oxfam: Translating Oxfam's Responsible Data Policy into practice, two years on* (The Engine Room and Oxfam 2017) <<https://oxfamlibrary.openrepository.com/oxfam/bitstream/10546/620257/1/rr-responsible-data-at-oxfam-190417-en.pdf>> accessed 22 June 2018

UNFPA, 'Guidelines on Data Issues in Humanitarian Crisis Situations' (UNFPA 2010)

<www.unfpa.org/sites/default/files/pub-pdf/guidelines_dataissues.pdf> accessed 22 June 2018

UNICEF, 'Fact Sheet: The Right to Participation' (UNICEF) <www.unicef.org/crc/files/Right-to-Participation.pdf> accessed 21 June 2018

UNICEF, Ethical Principles, Dilemmas and Risks in Collecting Data on Violence against Children: A review of Available Literature' (UNICEF 2012) <https://data.unicef.org/wp-content/uploads/2015/12/EPDRCLitReview_193.pdf> accessed 22 June 2018

United Nations Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (United Nations 2016) <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 21 June 2018

WFP Office of the Inspector General, 'Internal Audit of Beneficiary Management: Internal Audit Report AR/17/17' (WFP 2017) <<https://docs.wfp.org/api/documents/WFP-0000040084/download/>> accessed 21 June 2018

World Bank, 'Community Involvement and the Role of Nongovernmental Organizations in Environmental Assessment' (World Bank 1999) <http://siteresources.worldbank.org/INTSAFEPOL/1142947-1118039086869/20526287/Chapter7CommunityInvolvementAndTheRoleOfNGOsInEA.pdf>> accessed 21 June 2018

News Articles

-- 'Audit exposes UN food agency's poor data-handling' *IRIN News* (Geneva, 18 January 2018)

(Bekka Valley, 2 November 2016) <www.irinnews.org/feature/2016/11/02/aid%E2%80%99s-cash-revolution-numbers-game> accessed 21 June 2018

--, 'Cambridge Analytica: Facebook data-harvest firm to shut' *BBC* (2 May 2018) <www.bbc.com/news/business-43983958> accessed 16 June 2018

--, 'Syrian Aid in the Tech Age' *IRIN News* (Amman, 14 November 2013) <www.irinnews.org/report/99127/syrian-aid-tech-age> accessed 22 June 2018.

<www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling> accessed 21 June 2018

Goldman BP, Loeb R, and Tabatabai ES, 'The CLOUD Act, Explained' (*Orrick*, 6 April 2018) <www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained>

Nakashima E, 'Supreme Court to hear Microsoft case: A question of law and borders' *The Washington Post* (Washington, February 25 2018) <www.washingtonpost.com/world/national-security/supreme-court-case-centers-on-law-enforcement-access-to-data-held-overseas/2018/02/25/756f7ce8-1a2f-11e8-b2d9-08e748f892c0_story.html?utm_term=.8ee2b53555eb> accessed 17 June 2018

Parker B, 'Aid's cash revolution: a numbers game' *IRIN News*

Skahill E, 'Head in THE Cloud(s): What the U.S. v. Microsoft Case reveals about the Governmental Ramifications of Cloud Computing' *Brown Political Review* (7 April 2018)

<www.brownpoliticalreview.org/2018/04/head-clouds-u-s-v-microsoft-case-reveals-governmental-ramifications-cloud-computing/> accessed 21 June 2018

Websites

- 'Dataset' (*Cambridge Dictionary*) <<https://dictionary.cambridge.org/fr/dictionnaire/anglais/dataset>> accessed 22 June 2018
- ,'OCHA HDX Terms of Service' (*The Humanitarian Data Exchange*) <<https://data.humdata.org/about/terms>> accessed 16 June 2018
- 'The Right to Decide: the importance of respecting free, prior, and informed consent' (*Amazon watch*, 2011) <<http://amazonwatch.org/assets/files/fpic-the-right-to-decide.pdf>> accessed 21 June 2018
- 'Crowdsourcing' (Merriam-Webster, 28 May 2018) <www.merriam-webster.com/dictionary/crowdsourcing> accessed 22 June 2018
- , 'Data protection Laws of the world' (*DLA Piper*, 2018) <www.dlapiperdataprotection.com> accessed 17 June 2018
- 'Regulations, Directives, and other Acts' (*European Union*, 22 June 2018) <https://europa.eu/european-union/eu-law/legal-acts_en> accessed 22 June 2018.
- Dunmore C, 'Iris scan system provides cash lifeline to Syrian refugees in Jordan' (*UNHCR*, 23 March 2015) <www.unhcr.org/news/latest/2015/3/550fe6ab9/iris-scan-system-provides-cash-lifeline-syrian-refugees-jordan.html> accessed 21 June 2018
- Gough T, 'Fair and lawful processing: a hard lesson for charities, and what to do next' (*Linkedin*, 9 December 2016) <www.linkedin.com/pulse/fair-lawful-processing-hard-lesson-charities-what-do-next-tim-gough> accessed 21 June 2018
- Granryd M, 'Five ways mobile technology can help in humanitarian emergencies' (*World Economic Forum*, 22 August 2017) <www.weforum.org/agenda/2017/08/mobile-technology-humanitarian-crisis/> accessed 21 June 2018
- Matsakis L, 'Microsoft's Supreme Court Case has Big Implications for Data' (*Wired*, 27 February 2018) <www.wired.com/story/us-vs-microsoft-supreme-court-case-data/> accessed 17 June 2018
- NYC Taxi and Limousine Commission, 'NYC Taxi Trip Data 2013' (*FOIA/FOIL*) <<https://archive.org/details/nycTaxiTripData2013>> accessed 21 June 2018
- Pandurangan V, 'On Taxis and Rainbows: Lessons from NYC's improperly anonymized taxi logs' (*Tech Vijayp*, 21 June 2014) <<https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1>> accessed 21 June 2018
- Pratt MK, 'Big Data's Big Role in Humanitarian Aid' (*Computerworld*, 6 February 2016) <www.computerworld.com/article/3027117/big-data/big-datas-big-role-in-humanitarian-aid.html> accessed 16 June 2018
- Rouse M, 'Definition: Data Life Cycle' (*Whatis*, July 2017) <<https://whatis.techtarget.com/definition/data-life-cycle>> accessed 22 June 2018
- UN Global Pulse, 'Privacy and Data protection Principles: Towards a Responsible Governance' (*UN Global Pulse*) <www.unglobalpulse.org/privacy-and-data-protection-principle> accessed 22 June 2018