HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION

Co-editors: Christopher Kuner and Massimo Marelli

VUB BRUSSELS PRIVACY HUB

ICRC

REFERENCE

ICRC

International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01 F +41 22 733 20 57
E-mail: shop@icrc.org www.icrc.org
© ICRC, July 2017

Illustrations: The Value Web/Housatonic

HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION

Co-editors: Christopher Kuner and Massimo Marelli

Table of Contents

Acknowledgements

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

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

The drafting team comprised:

Christopher Kuner, Vagelis Papakonstantinou, Lina Jasmontaite, Ioulia Konstantinou and Amy Weatherburn, VUB;

Massimo Marelli, Pierre Apraxine and Romain Bircher, ICRC;

Catherine Lennman, Swiss Data Protection Authority;

Alba Bosch, European Data Protection Supervisor;

Caroline Dulin Brass, Office of the United Nations High Commissioner for Refugees (UNHCR);

Christina Vasala Kokkinaki, International Organization for Migration (IOM); and

Leslie Haskell, International Federation of Red Cross and Red Crescent Societies (IFRC).

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

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

Foreword

Jean-Philippe Walter, Deputy Swiss Federal Data Protection and Information Commissioner

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

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

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

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

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

Jean-Philippe Walter is also president of the French-speaking Association of Personal Data Protection Authorities and coordinator of the working group on the Resolution on Privacy and International Humanitarian Action.

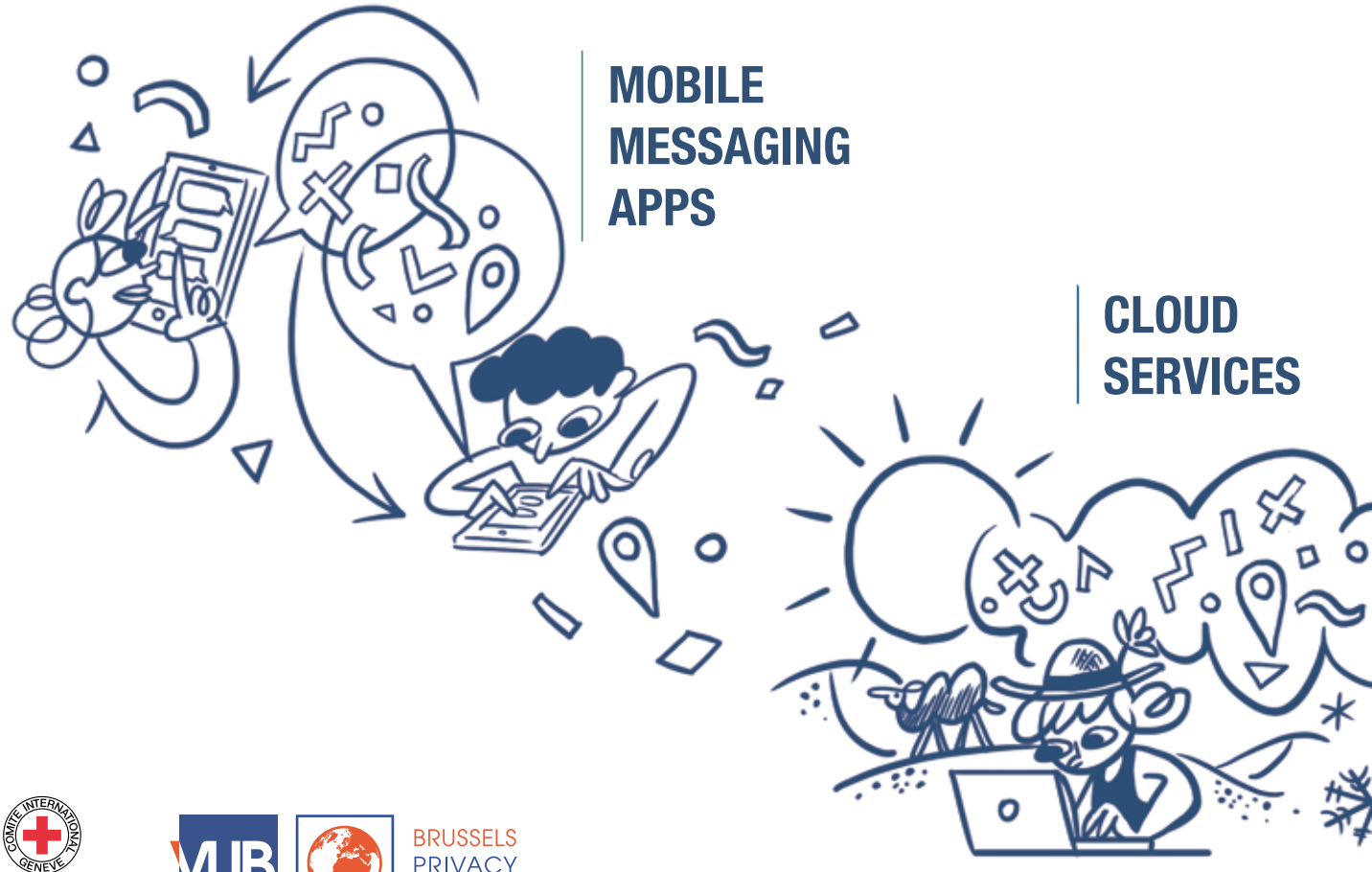
Glossary of defined terms and abbreviations

- **Anonymization** encompasses techniques that can be used to ensure that data sets containing Personal Data are fully and irreversibly anonymized so that they do not relate to an identified or identifiable natural person, or that the Data Subject is not or no longer identifiable.
- **Biometrics** or biometric recognition means the automated recognition of individuals based on their biological and behavioural characteristics.
- **Cash Transfer Programme** or programming, cash assistance intervention and cash-based assistance are terms in the humanitarian sector to describe the delivery of humanitarian aid in the form of vouchers or cash.
- **CERT** – Computer Emergency Response Team
- **CISO** – Chief Security Information Officer
- **Consent** means the freely-given, specific and informed indication of a Data Subject's wishes by which the Data Subject signifies agreement to Personal Data relating to him or her being processed.
- **CSIRT** – Computer Security Incident Response Team
- **CSO** – Chief Security Officer
- **CTO** – Chief Technical Officer
- **Data Analytics** denotes the practice of combining very large volumes of diversely sourced information (Big Data) and analysing them, using sophisticated algorithms to inform decisions.
- **Data Controller** means the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data.
- **Data Processor** means the person or organization who processes Personal Data on behalf of the Data Controller.
- **Data Protection Impact Assessment** or DPIA means an assessment that identifies, evaluates and addresses the risks to Personal Data arising from a project, policy, programme or other initiative.
- **Data Subject** means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to Personal Data.
- **DPO** in the context of this Handbook means a Humanitarian Organization's internal data protection office or data protection officer.
- **Drones** are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS).
- **Further Processing** means additional Processing of Personal Data that goes beyond the purposes originally specified at the time the data were collected.
- **Health Data** means data related to the physical or mental health of an individual, which reveal information about his/her health status.
- **Humanitarian Action** means any activity undertaken on an impartial basis to carry out assistance, relief and protection operations in response to a Humanitarian Emergency. Humanitarian Action may include "humanitarian assistance", "humanitarian aid" and "protection".
- **Humanitarian Emergency** means an event or series of events (in particular arising out of armed conflicts or natural disasters) that poses a critical threat to the health, safety, security or wellbeing of a community or other large group of people, usually over a wide area.
- **Humanitarian Organization** means an organization that provides aid to alleviate human suffering, and/or protects life and health, and upholds human dignity during Humanitarian Emergencies in accordance with its mandate and/or mission.
- **IaaS** – Infrastructure as a Service

- **International Data Sharing** includes any act of transferring or making Personal Data accessible outside the country or International Organization where they were originally collected or processed, including both to a different entity within the same Humanitarian Organization or to a Third Party, via electronic means, the internet, or other means.
- **International Organization** means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
- **Know Your Customer (KYC)** is a process enabling businesses to check the identity of their customers in order to comply with regulations and legislation on money laundering and corruption.[1]
- **PaaS** – Platform as a Service
- **Personal Data** means any information relating to an identified or identifiable natural person.
- **Processing** means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination or erasure.
- **Pseudonymization**, as distinct from anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
- **SaaS** – Software as a Service
- **Sensitive Data** means Personal Data which, if disclosed, may result in discrimination against or the repression of the individual concerned. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific situations in which Humanitarian Organizations work and the possibility that some data elements could give rise to discrimination, setting out a definitive list of Sensitive Data categories in Humanitarian Action is not meaningful. Sensitivity of data as well as appropriate safeguards (e.g. technical and organizational security measures) have to be considered on a case-by-case basis.
- **SLA** – A service-level agreement is an official commitment between a service provider and a client, particularly for the provision of reliable telecommunications and internet services.
- **Sought Person** is a person unaccounted for, for whom a tracing operation has been launched.
- **Sub-Processor** is a person or organization that is engaged by a Data Processor to process Personal Data on its behalf.
- **Third Party** is any natural or legal person, public authority, agency or any other body other than the Data Subject, the Data Controller and the Data Processor.
- **TLS** – Transport Layer Security is a cryptographic protocol to provide privacy and data integrity between a client and a server over an internet connection.

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

DATA PROTECTION and HUMANITARIAN ACTION



ICRC
VUB
BRUSSELS PRIVACY HUB

DRONES

BIOMETRICS

CASH TRANSFER PROGRAMMING

Chapter 1:
INTRODUCTION[2]

2 As stated in the Acknowledgements section above, the drafting team for this Handbook comprised Massimo Marelli, Pierre Apraxine and Romain Bircher (ICRC); Christopher Kuner, Vagelis Papakonstantinou, Lina Jasmontaite, Ioulia Konstantinou and Amy Weatherburn (VUB); Catherine Lennman (Swiss Data Protection Authority); Alba Bosch (European Data Protection Supervisor); Caroline Dulin Brass (UNHCR); Christina Vasala Kokkinaki (IOM); and Leslie Haskell (IFRC). The co-editors of the Handbook were Christopher Kuner and Massimo Marelli. Where a chapter of this Handbook relies on specific contributions made by third parties, this is acknowledged in a footnote in the relevant chapter.

1.1 Background

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

In suggesting how data protection principles should be applied by Humanitarian Organizations, this Handbook builds on existing guidelines, working procedures and practices that have been established in Humanitarian Action in the most volatile environments and for the benefit of the most vulnerable victims of armed conflicts, other situations of violence, natural disasters, pandemics and other Humanitarian Emergencies (together "Humanitarian Emergencies"). Some of these guidelines, procedures and practices pre-date the advent and development of data protection laws, but they all are based on the principle of human dignity and the same concept of protection which underpin data protection law. These guidelines have been set out, notably, in the Professional Standards for Protection Work.[3]

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

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

This Handbook is published as part of the Brussels Privacy Hub and ICRC's Data Protection in Humanitarian Action project, which was organized jointly by the Brussels Privacy Hub, an academic research centre of the Vrije Universiteit Brussel (VUB) in Brussels, Belgium, and the ICRC Data Protection Office in Geneva, Switzerland. The content of the Handbook was developed in a series of workshops held in Brussels and Geneva in 2015-2016, with representatives from

3 ICRC, *Professional Standards for Protection Work Carried out by Humanitarian and Human Rights Actors in Armed Conflict and Other Situations of Violence*, 2nd ed., Geneva 2013: https://www.icrc.org/en/publication/0999-professional-standards-protection-work-carried-out-humanitarian-and-human-rights, all internet references accessed in March 2017.

Humanitarian Organizations (including humanitarian practitioners), data protection authorities, academics, non-governmental organizations, researchers and other experts on specific topics. They came together to address questions of common concern in the application of data protection in Humanitarian Action, particularly in the context of new technologies. The individuals who participated in the various workshops are listed in Appendix II.

1.2 Objective

This Handbook aims to further the discussion launched by the International Conference of Data Protection and Privacy Commissioners' (ICDPPC's) Resolution on Privacy and International Humanitarian Action[4] adopted in Amsterdam in 2015. It is not intended to replace compliance with applicable legal norms, or with data protection rules, policies and procedures that a particular organization may have adopted. Rather, the Handbook seeks to raise awareness and assist Humanitarian Organizations in ensuring that they comply with Personal Data protection standards in carrying out humanitarian activities, by providing specific guidance on the interpretation of data protection principles in the context of Humanitarian Action, particularly when new technologies are employed.

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

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

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

- UN General Assembly Resolution 45/95 of 14 December 1990[5] adopting the *Guidelines for the Regulation of Computerized Personal Data Files,*[6] which includes the humanitarian clause calling for particular care and flexibility when applying data protection principles in the humanitarian sector;
- the *International Standards on the Protection of Personal Data and Privacy* (The Madrid Resolution) adopted by the ICDPPC in Madrid in 2009;[7]
- *The OECD Privacy Framework* (2013);[8] and
- the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), including the Additional Protocol.[9]

4 International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

5 UN General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95 14 December 1990: http://www.un.org/documents/ga/res/45/a45r095.htm.

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

7 International Conference on Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy:* https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf.

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

9 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing

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

- recent regulatory developments, insofar as they reflect further development of data protection concepts and principles in light of their application over the years and the challenges generated by new technologies (this includes the updating of Convention 108, as well as the EU General Data Protection Regulation 2016/679 (GDPR));[10]
- the Resolution on Data Protection and Major Natural Disasters[11] adopted by the ICDPPC in Mexico City in 2011;
- the Resolution on Privacy and International Humanitarian Action adopted by the ICDPPC in Amsterdam in 2015;[12]
- the ICRC *Rules on Personal Data Protection* (2015);[13]
- the ICRC *Professional Standards for Protection Work* (2013);[14]
- the UNHCR *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (2015);[15] and
- the *IOM Data Protection Manual* (2010).[16]

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

A few important considerations should be highlighted from the outset:

- The right to privacy has long been recognized globally as a human right,[17] while the right to Personal Data protection is a relatively recent human right that is closely connected to the right to privacy and sets forth conditions for the Processing of data of an identified or identifiable individual. More than 100 specific data protection laws and norms have been adopted at national and regional levels in recent years,[18] and Personal Data protection as a fundamental right is gaining wider acceptance around the world. Accordingly, implementation of Personal Data protection standards, even where not a legal obligation given the privileges and immunities enjoyed by certain Humanitarian Organizations, should be a priority for all Humanitarian Organizations, considering that the main objective of their activities is to work for the safety and dignity of individuals.
- Some Humanitarian Organizations are International Organizations enjoying privileges and immunities and not subject to national legislation. Respect for privacy and data protection rules is nevertheless, in many cases, a prerequisite for them to receive Personal Data from other entities.

---

of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

10 EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (EU General Data Protection Regulation), [2016] OJ L119/1.

11 International Conference on Data Protection and Privacy Commissioners, Resolution on Data Protection and Major Natural Disasters: https://icdppc.org/document-archive/adopted-resolutions/.

12 International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf.

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

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

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

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

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

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

- The exceptional emergency circumstances in which Humanitarian Organizations operate create special challenges regarding data protection. Accordingly, particular care and flexibility is required when applying data protection principles in the humanitarian sector. This need is also reflected in many of the international instruments and standards mentioned above, which include stricter rules for the Processing of Sensitive Data.[19]
- The lack of a uniform approach in data protection law to the Personal Data of deceased individuals means that Humanitarian Organizations should adopt their own policies on this matter (for example, by applying the rules applicable to the Personal Data of natural persons to the deceased, insofar as this makes sense). For organizations that do not enjoy immunity from jurisdiction, this question may be regulated by the applicable law.
- The focus of this Handbook is on Personal Data protection, and the application of this area of law to Humanitarian Action. Yet, in armed conflicts and other situations of violence, many threats are collective rather than individual – a village, a community, a specific group of men and women may share the same threats. So just focusing on the proper management of Personal Data may not be sufficient. In some cases, Processing of non-Personal Data may raise specific threats at the collective level. In this respect, a number of initiatives in the humanitarian sector have been focusing on the implications of Processing data more generally for communities and referring, for example, to "demographically identifiable information",[20] or "Community Identifiable Information".[21]
- Humanitarian Organizations process the Personal Data of different categories of individuals in Humanitarian Emergencies, such as data of beneficiaries and contacts involved in their activities, as well as data of staff and goods/service providers, or even data of donors. While the focus of this Handbook is the Processing of beneficiaries' Personal Data, similar considerations apply to the handling of Personal Data of other categories of individuals.

1.3 Structure and approach

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

1.4 Target audience

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

19 See Section 2.2. Basic data protection concepts.
20 See The Signal Code – A Human Rights Approach to Information During Crisis: https://signalcode.org/.
21 See Humanitarian Data Exchange Initiative: https://data.humdata.org/about/terms.

Chapter 2:
BASIC PRINCIPLES OF DATA PROTECTION

2.1 Introduction

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

An individual's right to Personal Data protection is not an absolute right. It should be considered in relation to the overall objective of protecting human dignity, and be balanced with other fundamental rights and freedoms, in accordance with the principle of proportionality.[22]

As the activities of Humanitarian Organizations are carried out primarily in Humanitarian Emergencies, they operate in situations where the protection of the Personal Data of beneficiaries and staff is often necessary to safeguard their security, lives and work. Accordingly, Personal Data protection and Humanitarian Action are complementary and reinforce each other. However, there may also be instances of friction where a balance between different rights and freedoms needs to be struck (e.g. between the freedom of expression and information and the right to data protection, or between the right to liberty and security of a person and the right to data protection). The human rights framework aims to ensure respect for all human rights and fundamental freedoms by balancing different rights and freedoms on a case-by-case basis. This approach often requires teleological interpretation of rights,[23] i.e. one that prioritizes the purposes the rights serve.

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

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

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

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

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

For example, it may be necessary to balance, on the one hand, data protection rights with, on the other hand, the objective of ensuring the historical and humanitarian accountability of stakeholders in Humanitarian Emergencies. Indeed, in Humanitarian Emergencies, Humanitarian Organizations may be the only external entities present, and may be the only possibility for future generations to have an external account of history as well as to provide a voice to victims.[24] Furthermore, data from Humanitarian Organizations may also be needed to support the victims of armed conflicts and other situations of violence or their descendants, for example in documenting their identity and legal status, submitting claims of reparations, etc. Data retention by Humanitarian Organizations may be of fundamental importance particularly considering that in Humanitarian Emergencies few or no other records may be available.

Confidentiality may also be of fundamental importance for some Humanitarian Organizations, as it may be an essential precondition for the ongoing viability of Humanitarian Action in volatile environments, to ensure acceptance by parties to a conflict and people involved in other situations of violence, proximity to people in need and the safety of their staff. This may have an impact, for example, on the extent to which Data Subject access rights may be exercised.[25]

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

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

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

2.2 Basic data protection concepts[26]

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

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

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

Some data protection laws include the additional category of **Sensitive Data** in the concept of Personal Data. For the purposes of the present Handbook, Sensitive Data means Personal Data, which if disclosed, may result in discrimination against or the repression of an individual. Typically, data relating to health, race or ethnicity, religious/political/armed group affiliation, or genetic and biometric data are considered to be Sensitive Data. All Sensitive Data require augmented protection even though different types of data falling under the scope of Sensitive Data (e.g. different types of biometric data) may present different levels of sensitivity. Given the specific environments in which Humanitarian Organizations work and the possibility that various data elements may give rise to discrimination, setting out a definitive list of Sensitive Data categories

26 The terms defined below are also given in the Glossary at the beginning of the Handbook.

for Humanitarian Action is not meaningful. For example, in some situations, a simple list of names may be very sensitive, if it puts the individuals on the list and/or their families at risk of persecution. Equally, in other situations, data collected to respond to Humanitarian Emergencies may need to include data that in a regular data protection context would be considered to be Sensitive Data and the Processing of such data would be, in principle, prohibited, but in the local culture and the specific circumstances may be relatively harmless. Therefore, it is necessary to consider the sensitivity of data and the appropriate safeguards to protect Sensitive Data (e.g. technical and organizational security measures) on case-by-case basis.

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

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

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

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

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

2.3 Aggregate, Pseudonymized and Anonymized data sets

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

Where aggregate data are derived from Personal Data, and could in certain circumstances pose risks to persons of concern, it is important to ensure that the Processing, sharing, and/or publication of such data cannot lead to the re-identification of individuals.[27]

Although specific Consent from Data Subjects is not required for their Personal Data to be used in aggregate data sets or statistics, Humanitarian Organizations should ensure that such data Processing has another legitimate basis,[28] and does not expose individuals or groups to harm, or otherwise jeopardize their protection.

The Anonymization of Personal Data can help meet the protection and assistance needs of vulnerable individuals in a privacy-friendly way. The term "Anonymization" encompasses techniques that can be used to convert Personal Data into anonymized data. When anonymizing data, it is essential to ensure that data sets containing Personal Data are fully and irreversibly anonymized. Anonymization processes are challenging where large data sets containing a wide range of Personal Data are concerned and may pose a greater risk of re-identification.[29]

"Pseudonymization", as distinct from Anonymization, means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person. This may involve replacing the anagraphic[30] data in a data set with a number. Sharing registration/identification numbers instead of names is good practice, but does not amount to Anonymization.

Prior to sharing or publicising anonymized data, it is important to ensure that no Personal Data are included in the data set and that individuals cannot be re-identified. The term "re-identification" describes the process of turning allegedly anonymized data back into Personal Data through the use of data matching or similar techniques.[31] If the risk of re-identification is deemed to be reasonably likely, the information should be considered to be Personal Data and subject to all the principles and guidance set out in this Handbook. It can be very difficult to assess the risk of re-identification with absolute certainty.

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

2.4 Applicable law and International Organizations

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

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

28 See Chapter 3: Legal bases for Personal Data Processing.

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

30 https://en.wiktionary.org/wiki/anagraphic.

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

them to perform the mandate attributed them by the community of states under international law in full independence.

As far as NGOs are concerned, the rules for determining applicable data protection law depend on a number of different factual elements. This Handbook does not deal with issues of applicable law; any questions in this regard should be directed to the NGO's legal department or data protection office (DPO).[32]

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

International Organizations enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence and are not covered by the jurisdiction of the countries in which they work. They can therefore process Personal Data according to their own rules, subject to the internal monitoring and enforcement of their own compliance systems; in this regard they constitute their own "jurisdiction". This aspect of International Organizations has specific implications, in particular for International Data Sharing, which will be discussed in detail in Chapter 4: International Data Sharing.

2.5 Data Processing principles

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

2.5.1 The principle of the fairness and lawfulness of Processing

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

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

32 See Section 1.2 Objective.

2.5.2 The purpose limitation principle

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

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

Humanitarian Organizations should take care to consider and identify at the outset of data collection (and as much as possible in emergency circumstances) all possible purposes contemplated and that may be contemplated in any Further Processing, so as to be as transparent as possible.

2.5.3 The principle of proportionality

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

The data handled by Humanitarian Organizations should be adequate, relevant and not excessive for the purposes for which they are collected and processed. This requires, in particular, ensuring that only the Personal Data that are necessary to achieve the purposes (fixed in advance) are collected and further processed and that the period for which the data are stored, before being anonymized or deleted, is limited to the minimum necessary.[33]

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

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

33 See Section 2.7 Data retention.

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

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

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

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

2.5.4 The principle of data minimization

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

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

- Has the specified purpose been achieved?
- If not, are all data still necessary to achieve it? Is the specified purpose so unlikely to be achieved that retention no longer makes sense?
- Have inaccuracies affected the quality of Personal Data?
- Have any updates and significant changes rendered the original record of Personal Data unnecessary?

- Are the data necessary for legitimate historical, statistical, or scientific purposes? Is it proportionate to continue storing them, taking into account the associated risks? Are appropriate data protection safeguards applied to this further storage?
- Have the Data Subject's circumstances changed, and do these new factors render the original record obsolete and irrelevant?

2.5.5 The principle of data quality

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

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

2.6 Special data Processing situations

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

2.6.1 Health purposes

Improper handling (including disclosure) of Health Data could cause significant harm to the individuals concerned. Accordingly, Health Data should be considered as particularly sensitive and specific guarantees should be implemented when Processing such data. This also applies to Sensitive Data. Health Data are also increasingly becoming a target for cyber-attacks. Humanitarian healthcare providers should process data in accordance with the WMA International Code of Medical Ethics[34] which includes specific professional obligations of confidentiality.

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

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

Health Data should be kept separate from other Personal Data, and should only be accessible by healthcare providers or personnel specifically delegated by the humanitarian healthcare providers to manage Health Data under confidentiality guarantees ensured by employment, consultant, research or other contracts.

34 World Medical Association, *WMA International Code of Medical Ethics*: http://www.wma.net/en/30publications/10policies/c8/.

Humanitarian Organizations engaged in protection or assistance activities may also process Health Data, for example, when this is necessary to locate persons unaccounted for (where Health Data may be required to identify and trace them) or to advocate for adequate treatment of individuals deprived of their liberty, or for the establishment of livelihood programmes addressing the needs of particularly vulnerable categories of beneficiaries (such as people suffering from malnutrition or particular diseases).[35]

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

2.6.2 Administrative activities

Humanitarian Organizations typically process Personal Data for employment purposes, career management, assessments, direct marketing and other administrative requirements. In some instances this may also include sensitive Processing activities such as, for example, GPS tracking of its vehicles for fleet and security management.

2.6.3 Further Processing

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

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

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

35 See Section 2.6.3 Further Processing.

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

Consequently, the purposes strictly linked to Humanitarian Action, and which do not incur any additional risks unforeseen in the consideration of the initial purpose, are likely to be compatible with each other and, if this is confirmed, Personal Data can legitimately be processed by Humanitarian Organizations beyond the specific purposes for which the Personal Data were originally collected, as long as the Humanitarian Organization does so within the framework of Humanitarian Action. In principle, Further Processing should be permissible if this is necessary and proportionate to safeguard public security and the lives of affected individuals in Humanitarian Action. This requires a case-by-case assessment and cannot be presumed across the board.

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

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

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

Should the intended other purpose not be compatible with the purpose for which the data were initially collected, the data should not be further processed, unless it is deemed appropriate to do so under another legal basis.[36]

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

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

36 See Chapter 3: Legal bases for Personal Data Processing.

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

2.7 Data retention

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

When data have been deleted, all copies of the data should also be deleted. If the data have been shared with Third Parties, the Humanitarian Organization should take reasonable steps to ensure such Third Parties also delete the data. This consideration should be taken into account in initial reflections as to whether to share data with Third Parties and should be expressed in any data sharing agreement.[37]

2.8 Data security and Processing security

2.8.1 Introduction

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

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

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

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

37 See Section 2.12 Data sharing and International Data Sharing and Chapter 4: International Data Sharing.

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

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

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

The Data Controller is responsible for:

- Setting up an information security management system. This includes establishing and regularly updating a data security policy based on internationally accepted standards and on a risk assessment. The policy should consist of, for example, physical security guidelines, IT security policy, email security guidelines, IT equipment usage guidelines, guidelines for information classification (i.e. classifying information as public, internal, confidential and strictly confidential), a contingency plan, and document destruction guidelines.
- Developing the communication infrastructure and databases in order to preserve the integrity and security of data, in compliance with the security policy.
- Taking all appropriate measures to protect the security of data processed in the Data Controller's information system.
- Granting and administering access to databases containing Personal Data, including ensuring access is granted on a need-to-know basis.
- The security of the facilities which enable authorized personnel to access the system.
- Compliance with the security rules referred to in this Handbook.
- Ensuring that the personnel given access to data are in a position to fully respect security rules. This includes relevant training, a pledge of discretion and/or duty of confidentiality clause in the employment contract to be signed before access to databases is granted.
- Maintaining a register of personnel having access to each database, and updating it when appropriate (e.g. personnel being given different responsibilities who no longer require access).
- If feasible, keeping a historical log and potentially running audits of personnel having had access to a database, for as long as the data processed by such personnel are present in the database.

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

2.8.2 Physical security

Each Data Controller is responsible for:

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

2.8.3 IT security

The Data Controller should:

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

All email correspondence, internal and external, containing Personal Data should be processed on a need-to-know basis. Recipients of email correspondence should be carefully selected to avoid unnecessary dissemination of Personal Data. Private email accounts should not be used to transfer Personal Data.

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

Staff members handling Personal Data should take due care when connecting remotely to the Data Controller's servers. Passwords should always be protected, regularly changed and not be automatically entered through 'keychain' functions.[38] Staff should check that they have logged off properly from computer systems and that open browsers have been closed.

Laptops, smartphones and other portable media equipment require special safety precautions, especially when working in a difficult environment. Portable media equipment should be stored in safe and secure locations at all times.

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

Effective recovery mechanisms and backup procedures should cover all electronic records, and the relevant information and communications technology

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

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

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

2.8.4 Duty of discretion and staff conduct

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

- All personnel and external consultants signing discretion and confidentiality agreements or clauses as part of their employment/consulting contract. This requirement goes together with the requirement that personnel should only process data in accordance with the Data Controller's instructions.
- Any external Data Processor being contractually bound by confidentiality clauses. This requirement goes together with the requirement that the Data Processor should only process data in accordance with the Data Controller's instructions.
- The strict application of the guidelines for information classification based on their confidentiality status.
- Ensuring that any request by Data Subjects that their Personal Data be processed in a particular way and, in particular, that it be considered confidential and not shared with Third Parties, is accurately recorded in the file of the Data Subject.
- In order to limit the risk of leaks, only authorized personnel should be in charge of the collection and management of data from confidential sources, and have access to documents according to the applicable guidelines for information classification.

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

2.8.5 Contingency planning

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

2.8.6 Destruction methods

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

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

The Controller should conduct a sensitivity assessment prior to destruction to ensure that appropriate methods of destruction are used to eliminate Personal Data. In this regard, the following three paragraphs are based on information taken from the IOM Data Protection Manual:[39]

39 International Organization for Migration (IOM), *Data Protection Manual*, 2010, pages 83-84: https://publications.iom.int/books/iom-data-protection-manual.

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

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

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

2.8.7 Other measures

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

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

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

2.9 The principle of accountability

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

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

- drafting of Personal Data Processing policies (including Processing Security policies);
- keeping internal records of data Processing activities;
- creating an independent body to oversee the implementation of the applicable data protection rules, such as a Data Protection Office, and appointment of a Data Protection Officer (DPO);
- implementing data protection training programmes for all staff;
- performing Data Protection Impact Assessments (DPIAs);[40] and
- registering with the competent authorities (including data protection authorities), if legally required and not incompatible with the principle of "do no harm".

2.10 Information

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

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

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

2.10.1 Data collected from the Data Subject

Personal Data may be collected directly from the Data Subject under the following legal bases:[41]

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

The types of information to be provided to Data Subjects in each of the above cases will vary depending on the particular circumstances. A priority in this respect is that the information provided must be sufficient to enable them to exercise their data protection rights effectively.[42]

2.10.2 Information notices

In the specific cases where Consent may be used as the legal basis,[43] the individual must be put in a position to fully appreciate the risks and benefits of data Processing, otherwise Consent may not be considered valid.

40 See Chapter 5 Data Protection Impact Assessments (DPIAs).
41 See Chapter 3: Legal bases for Personal Data Processing.
42 See Section 2.11 Rights of Data Subjects.
43 See Section 3.2 Consent.

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

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

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

- the identity and contact details of the Data Controller;
- the specific purpose for Processing of his/her Personal Data;
- who to contact in case of any questions concerning the Processing of their Personal Data; and
- with whom the data will be shared, in particular if it may be shared with authorities (e.g. law enforcement authorities) or entities in another territory or jurisdiction.

Additional information must be provided where necessary to enable individuals to Consent and exercise their rights of access, objection, rectification, erasure and/or if the Data Subject requests more information.[44]

In exceptional circumstances where, due to prevailing security and logistical constraints, including difficulties gaining access to the field, it is not possible to provide this information immediately or at the place where individuals are located, or where the data have not been collected directly from the Data Subject, the information should be made available as soon as possible in a way that is easy for individuals to access and understand.[45] Humanitarian Organizations should also refrain from collecting extensive data sets from beneficiaries until

44 See Section 2.10 Information and Section 3.2 Consent.
45 See Section 2.10 Information.

this information can be adequately provided, unless absolutely necessary for humanitarian purposes.

2.10.3 Data not collected from the Data Subject

Where the Personal Data have not been obtained from the Data Subject, the information set out under Section 2.10.2 above, depending on the legal basis used for the collection of data, should be provided to the Data Subject within a reasonable period after obtaining this data, having regard to the specific circumstances in which the data are processed or, if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed, subject to logistical and security constraints.

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

2.11 Rights of Data Subjects

2.11.1 Introduction

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

An individual should be able to exercise these rights using the internal procedures of the relevant Humanitarian Organization, such as by lodging an inquiry or complaint with the organization's DPO. However, depending on the applicable law, and in cases where the Data Controller is not an International Organization with immunity from jurisdiction, the individual may also have the right to bring a claim in court or with a data protection authority. In the case of International Organizations, claims may be brought before an equivalent body responsible for independent review of cases for the organization.[46]

2.11.2 Access

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

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

The Humanitarian Organization's staff should not reveal any information relating to Data Subjects, unless they are provided with proof of identify satisfying them that the Data Subjects are who they say they are.

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

Access to documents does not apply when overriding interests require that access not be given. Thus, compliance by Humanitarian Organizations with a Data Subject's access request may be restricted as a result of the overriding public interests or interests of others. This is particularly the case where access cannot be provided without revealing the Personal Data of others, unless the document or information can be meaningfully redacted to blank out any reference to such other Data Subjects or such other Data Subjects have consented to the disclosure, without disproportionate effort. This is always the case when access would jeopardize the ability of a Humanitarian Organization to pursue the objectives of its Humanitarian Action or when it creates risks for the security of its staff. This may also be the case for internal documents of the Humanitarian Organizations, disclosure of which may have an adverse effect on Humanitarian Action.

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

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

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

* UN Security Council Resolution 1244.

2.11.3 Correction

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

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

2.11.4 Right to erasure

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

- the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed and/or further processed; or,
- the Data Subject has withdrawn his/her Consent for Processing, and there is no other basis for the Processing of the data;[47] or
- the Data Subject successfully objects to the Processing of Personal Data concerning him/her;[48] or
- the Processing does not comply with the applicable data protection and privacy laws, regulations and policies.

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

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

2.11.5 Right to object

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

47 See Section 3.2 Consent.
48 See Section 3.4 Important grounds of public interest and Section 3.5 Legitimate interest.

The exercise of this right may be restricted if necessary for the protection of the Data Subject or the rights and freedoms of others, for the documentation of alleged violations of international humanitarian law or human rights law or for legitimate historical or research purposes, subject to appropriate safeguards and taking into account the risks for and the interests of the Data Subject. In these cases, the Humanitarian Organization should:

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

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

2.12 Data sharing and International Data Sharing

Humanitarian Emergencies routinely require Humanitarian Organizations to share Personal Data with Data Processors and Third Parties, including those based in other countries, or with International Organizations. Data protection laws restrict the sharing of and access to Personal Data with Third Parties, in particular in case of transfers across borders or jurisdictions. Also, many data protection laws restrict International Data Sharing, which means any act of making Personal Data accessible outside the country in which they were originally collected or processed, as well as to a different entity within the same Humanitarian Organization not enjoying the status of International Organization, or to a Third Party, via electronic means, the internet, or others.[49]

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

49 See Chapter 4: International Data Sharing.

Chapter 3:

LEGAL BASES FOR PERSONAL DATA PROCESSING

3.1 Introduction

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

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

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

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

Processing by Humanitarian Organizations may often be based on vital interest or on important grounds of public interest,[50] i.e. in the performance of a mandate established under national or international law. This would require that the following conditions be met:

- In the case of vital interest, having sufficient elements to consider that in the absence of Processing the individual could be at risk of physical or moral harm. In the case of important grounds of public interest, being clear that the specific Processing operation is within a mandate established for the Humanitarian Organization under national, regional or international law.
- Providing clear information to the individual as to the proposed Processing operation.
- Ensuring the individual has a say and is in a position to exercise the right to object.[51] In any case, the opportunity to object to the Processing should be offered as soon and as clearly as possible, preferably at the moment of data collection. If the Data Subject objects to the Processing on legitimate grounds, the Processing should not involve data relating to that person, unless any of the exceptions below apply (e.g. Section 3.3 Vital interest or Section 3.4 Important Grounds of Public interest).

Relying on an appropriate legal basis does not discharge a Humanitarian Organization of its responsibility to assess the risk, for an individual, a given group, or the Humanitarian Organization itself of collecting, storing or using Personal Data. In cases involving particularly high risks, Humanitarian Organizations should consider whether it is not more appropriate to refrain from collecting and/or Processing the data in the first place. Such risks may be immediately evident from the Humanitarian Organization's experience or hidden in the complexity of the data flows inherent in a new technological solution. The performance of a Data Protection Impact Assessment (DPIA) therefore remains a key tool to ensure that all relevant risks are identified and mitigated.[52]

50 See Section 3.3 Vital interest and Section 3.4 Important Grounds of Public interest.
51 See Section 2.11.5 Right to object.
52 See Chapter 2: Basic principles of data protection.

3.2 Consent

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

- the Data Subject is not physically in a position to be informed and give free Consent, either because, for example, he/she is a Sought Person, or he/she is unconscious; or
- the Humanitarian Organization is not in a position to inform and obtain the Consent of the Data Subject due to the prevailing security or logistical conditions in the area of operations; or
- the Humanitarian Organization is not in a position to inform and obtain the Consent of the Data Subjects due to the scale of the operation that needs to be carried out. This can be the case, for example, (i) when preparing lists for distribution of humanitarian assistance to large numbers of displaced people, or (ii) when authorities provide Humanitarian Organizations with lists of protected persons, under a provision deriving from international humanitarian law or human rights law; or
- in the organization's assessment, the Consent of the Data Subject cannot be valid due, for example, to the Data Subject being particularly vulnerable (e.g. children, elderly or disabled persons) at the time of giving Consent, or having no real choice to refuse Consent due to a situation of need and vulnerability, including a lack of alternative to the specific assistance being offered and the data Processing involved; or
- when new technologies are involved, characterized by complex data flows and multiple stakeholders, including Data Processors and sub-Data Processors in multiple jurisdictions. This makes it difficult for an individual to fully appreciate the risks and benefits of a Processing operation and, therefore, take the responsibility for it as entailed by giving Consent. In this case, other legal bases, which require Humanitarian Organizations to take more responsibility for the assessment of risks and benefits of Processing, would be more appropriate.

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

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

3.2.1 Unambiguous

Consent should be given unambiguously by any appropriate method enabling a freely-expressed, specific and informed indication of the Data Subject's wishes by means of a written or, in the event that this is not possible, oral or other statement, or by another clear affirmative action by the Data Subject signifying their agreement to Personal Data relating to them being processed.

3.2.2 Timing

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

3.2.3 Validity

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

3.2.4 Vulnerability

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

Vulnerability varies depending on the circumstances. In this respect, the following factors should be considered:[53]

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

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

3.2.5 Children

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

53 International Organization for Migration (IOM), Data Protection Manual (2010), pages 45-48: https://publications.iom.int/books/iom-data-protection-manual.

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

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

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

3.2.6 Informed

Consent should be informed if it is to be accepted as the legal basis for Processing. This requires that the Data Subject receive explanations in simple, jargon-free language, which allows for full appreciation and understanding of the circumstances, risks, and benefits of Processing.[54]

3.2.7 Documented

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

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

54 See Section 2.10 Information.

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

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

3.2.8 Withholding/withdrawing Consent

If Data Subjects expressly withhold Consent, they should be advised about the implications, including the effect this may have on assistance that might or might not be rendered by Humanitarian Organizations and/or Third Party organizations. If, however, assistance could not be provided in the absence of Consent, note that Consent could not be considered as a legal basis for the Processing.[55]

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

3.3 Vital interest

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

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

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

55 See Section 3.2 Consent, fourth bullet point.

In these cases, however, the Humanitarian Organization should, if possible, ensure that the Data Subjects are aware of the Processing as soon as possible, that they have sufficient knowledge to understand and appreciate the specified purpose(s) for which Personal Data are collected and processed, and are in a position to object to the Processing if they so wish. This can be achieved preferably through direct explanations at the moment of the collection and, for example, during distributions of assistance, using posters, group explanations or by making further information available on leaflets or on web sites when beneficiaries are registered or aid is distributed.[56]

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

3.4 Important grounds of public interest

Important grounds of public interest are triggered when the activity in question is part of a humanitarian mandate established under national or international law. This for example would be the case for the ICRC, National Societies of the Red Cross/Red Crescent, the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations World Food Programme (WFP), the International Organization for Migration (IOM), and other Humanitarian Organizations mandated under national or international law to carry out specific tasks, in so far as the Processing of Personal Data is necessary to accomplish those tasks.[57] In this case, the term "necessary" is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,[58] to fulfil the relevant purpose).

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

Other scenarios where this legal basis may be relevant include the Processing of Personal Data of persons in detention, where this type of activity is within the mandate of the Humanitarian Organization in question. This may happen, for example, when the Processing of Personal Data relates to persons deprived of their liberty in an armed conflict or other situation of violence, where the Humanitarian Organization has not yet been in a position to visit the Data Subject deprived of liberty and therefore obtain his/her Consent and, subsequently, if Consent is not considered as a valid legal basis due to the vulnerability of the Data Subjects.

56 See Section 2.5.1 The principle of the fairness and lawfulness of Processing and Section 2.10 Information.
57 For example, the ICRC has a mandate under the four Geneva Conventions and Additional Protocol I to act in the event of international armed conflict. The ICRC has a right of humanitarian intervention in non-international armed conflicts: https://www.icrc.org/en/mandate-and-mission.
58 See example at Section 3.6 Performance of a contract.

Detainees in the Central Prison, Monrovia, Liberia.

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

3.5 Legitimate interest

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, in particular, when a specific humanitarian activity is listed in their mission, and provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. In all of these situations, the term "necessary" is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,[59] to fulfil the relevant purpose). Legitimate interest may include situations such as the following:

- The Processing is necessary for the effective performance of the Humanitarian Organization's mission, in cases where important grounds of public interest are not triggered due to the absence of a mandate under domestic or international law.
- The Processing is necessary for the purposes of ensuring information systems and information security,[60] and the security of the related services offered by, or accessible via, these information systems, by public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services and by providers of security technologies and services. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems.

59 See example at 3.6 Performance of a contract.

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

- The Processing is necessary for the purposes of preventing, evidencing and stopping fraud or theft.
- The Processing of Personal Data is necessary for the purposes of anonymizing or pseudonymizing Personal Data.[61]
- Where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial, administrative or any out-of-court procedure.

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

3.6 Performance of a contract

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

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

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

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

3.7 Compliance with a legal obligation

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

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

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

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

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

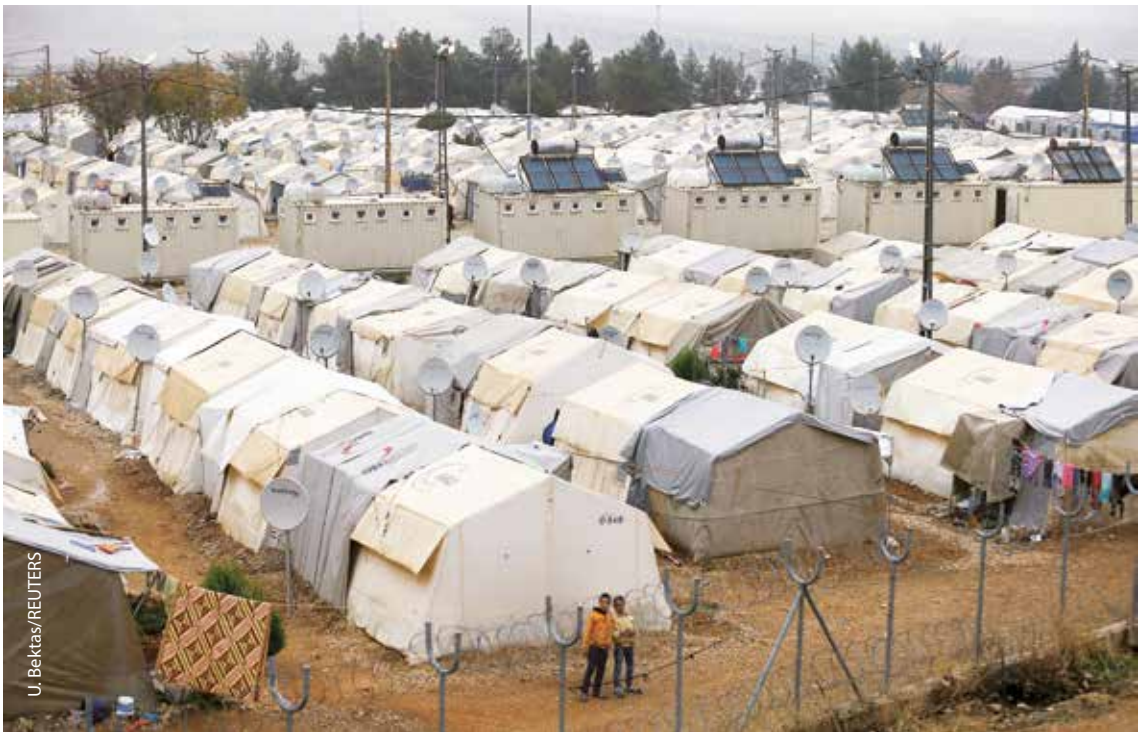
In this respect, it is also important to stress that Humanitarian Organizations should consider whether any legal obligation to disclose data applicable to them may put their Data Subjects at risk of repression, in which case they should consider not engaging in data collection in the first place.

Chapter 4:

INTERNATIONAL DATA SHARING

4.1 Introduction

Humanitarian Emergencies know no borders and regularly create the need for Humanitarian Organizations to share data with other entities across borders to provide the necessary humanitarian response. Accordingly, ensuring efficient cross-border flows of Personal Data between different countries is essential to the work of Humanitarian Organizations. In addition, the adoption of new technologies in humanitarian responses requires the involvement of multiple Data Processors and Sub-Processors which are, almost inevitably, established in various jurisdictions other than that where the Humanitarian Emergency takes place. This may be the case, for example, when cloud-based solutions are used by Humanitarian Organizations to process Personal Data, in which case data may be hosted in the territory where the organization is headquartered, and service providers may be acting as Data Processors and Sub-Processors in a number of jurisdictions.[62]



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

As discussed in Section 2.4 Applicable law and International Organizations, some Humanitarian Organizations are International Organizations which enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence. Accordingly, they process Personal Data according to their own rules, which apply across their work irrespective of the territory they operate in, and subject to the control of and enforcement by their own compliance systems. Thus, they constitute their own "jurisdiction", and data flows within them and their subordinate bodies do not fall within the scope of this Chapter.[63]

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

- offices within the same non-governmental organization (NGO) operating in different countries;
- other NGOs, International Organizations, and United Nations agencies;
- government authorities;

62 See Chapter 10: Cloud Services.
63 See Section 2.4 Applicable law and International Organizations.

- Data Processors such as service providers, consultants or researchers collecting and/or Processing Personal Data on behalf of the Humanitarian Organization;
- academic institutions and/or individual researchers;
- private companies; and
- museums.

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

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

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

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

It should not be forgotten that data sharing is a Processing operation and is therefore subject to all the requirements set out in the previous Chapters.[64] This Chapter explains the additional precautions Humanitarian Organizations should take whenever carrying out International Data Sharing.

4.2 Basic rules for International Data Sharing

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

- any data protection rules or privacy requirements applicable to the data sharing[65] (including any data protection or privacy requirements of local law, if applicable) have been satisfied prior to the transfer; and
- a legal basis must be provided for the transfer; and
- a DPIA should be carried out to determine that the transfer does not present unacceptable risks for the individual (e.g. discrimination or repression); and
- the organization that initiates the transfer must be able to demonstrate that adequate measures have been undertaken to ensure compliance with the data protection principles set forth in this Handbook by the recipient entity in order to maintain the level of protection of Personal Data with regard to International Data Sharing (accountability); and
- the individual should be informed about the recipient(s) of the transfer. The transfer should not be incompatible with the reasonable expectations of the individuals whose data are transferred.

64 See Chapter 2: Basic principles of data protection and Chapter 3: Legal bases for Personal Data Processing.
65 See Chapter 2: Basic principles of data protection.

4.3 Providing a legal basis for International Data Sharing

4.3.1 Introduction

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

4.3.2 Legal bases for International Data Sharing

International Data Sharing may be carried out:

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

These legal bases are used in similar ways to their application in Personal Data Processing.[66] In addition, as International Data Sharing involves additional risks, the factors listed below in the section on "Mitigating the risks to the individual" should be given due consideration.

4.4 Mitigating the risks to the individual

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

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

66 See Chapter 3: Legal bases for Personal Data Processing.

These last two factors are considered in more detail below.

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

4.4.1 Appropriate safeguards/Contractual clauses

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

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

The European Commission has issued standard contractual clauses for transfers from Data Controllers to Data Controllers and to Data Processors established outside the EU/EEA[67] for Humanitarian Organizations subject to EU data protection law or wishing to use these clauses.

Another factor to consider when deciding on risk mitigation is whether the other party involved in data sharing is committed to a code of conduct covering Personal Data Processing[68] and the extent to which such a code of conduct is applied in practice, whether it is binding and enforceable or not.
Even when a legal basis exists for the transfer and mitigating measures are put in place, it may not be appropriate to carry out International Data Sharing, because of factors such as the following:

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

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

67 See European Commission, Model Contracts for the transfer of personal data to third countries: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.
68 See for example, International Red Cross and Red Crescent Movement Restoring Family Links Network, Code of Conduct on Data Protection: https://www.icrc.org/en/document/rfl-code-conduct.

To identify and address or mitigate such risks properly, a DPIA should be carried out.[69] In case of doubt, the Humanitarian Organization's DPO should be consulted.

4.4.2 Accountability

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

- keeping internal records concerning data Processing and, in particular, a log of the transfer;
- appointment of a DPO;
- drafting of Personal Data Processing policies, including a data security policy;
- performing and keeping a record of the DPIA(s) relating to the transfer; and
- registration of the transfer with the competent authorities (i.e. data protection authorities), if required by applicable law.

For any International Data Sharing, appropriate measures should be used to safeguard the transmission of Personal Data to Third Parties. The level of security[70] adopted and the method of transmission should be proportionate to the nature and sensitivity of Personal Data and to the risks involved. It is also advisable to consider this factor as part of the DPIA to further specify the precautions to be taken.

4.5 Data Controller/Data Processor relationship

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

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

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

4.6 The disclosure of Personal Data to authorities

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

69 See Chapter 5: Data Protection Impact Assessments (DPIAs).
70 See Section 2.8 Data security and Processing security.

Humanitarian Organizations enjoying privileges and immunities as International Organizations should ensure that their specific status is respected and refuse to accede to such requests unless necessary in the best interest of the Data Subjects and Humanitarian Action. When a Humanitarian Organization enjoying privileges and immunities needs to transfer data to Humanitarian Organizations that do not enjoy such privileges and immunities, the risk that the recipient may not be in a position to resist such requests should be taken into account. This risk is specifically recognized in the International Conference of Privacy and Data Protection Commissioners' Resolution on Privacy and International Humanitarian Action of 2015:[71]

> *"Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to Humanitarian Action more generally."*

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

Chapter 5:

DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

5.1 Introduction

The Processing of Personal Data can increase risks for individuals, groups and organizations, as well as society as a whole. The purpose of a Data Protection Impact Assessment (DPIA)[72] is to identify, evaluate and address the risks to Personal Data arising from a project, policy, programme or other initiative. A DPIA should ultimately lead to measures that contribute to the avoidance, minimization, transfer or sharing of data protection risks. A DPIA should follow a project or initiative that requires Processing of individuals' data throughout its life cycle. The project should revisit the DPIA as it undergoes changes or as new risks arise and become apparent.

Here are examples of when a DPIA is appropriate:

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

Schermbrucker/UNICEF

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

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

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

This Chapter is a step-by-step guide for Humanitarian Organizations on how to conduct a DPIA and what should be included in a DPIA report. Appendix I contains a template for a DPIA report.[73] Although a DPIA report is not the end of a DPIA process, it is crucial to its success. It helps the Humanitarian Organization identify the privacy impacts of a proposed project and what must be done to ensure that the project protects Personal Data. It also helps the Humanitarian Organization reassure stakeholders that it takes their rights to privacy and data protection seriously and that it seeks the views of those who might be affected by or interested in the programme. Humanitarian Organizations should consider making the DPIA report or, at least, a summary of it available to stakeholders.

5.2 The DPIA process

This section provides a guide through the steps necessary to undertake a DPIA. There are different approaches to conducting DPIAs. The following guidance draws on best practices from a range of sources.[74]

5.2.1 Is a DPIA necessary?

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

5.2.2 The DPIA team

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

5.2.3 Describing the Processing of Personal Data

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

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

73 See Appendix I — Template for a DPIA report.

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

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

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

5.2.4 Consulting stakeholders

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

5.2.5 Identify risks

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

5.2.6 Assess the risks

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

- consult and deliberate with internal and/or external stakeholders to identify risks, threats and vulnerabilities;
- evaluate the risks against agreed risk criteria;[75]
- assess the risk in terms of likelihood and severity of impact; and
- assess against the necessity, suitability and proportionality tests.

5.2.7 Identify solutions

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

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

5.2.8 Propose recommendations

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

5.2.9 Implement the agreed recommendations

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

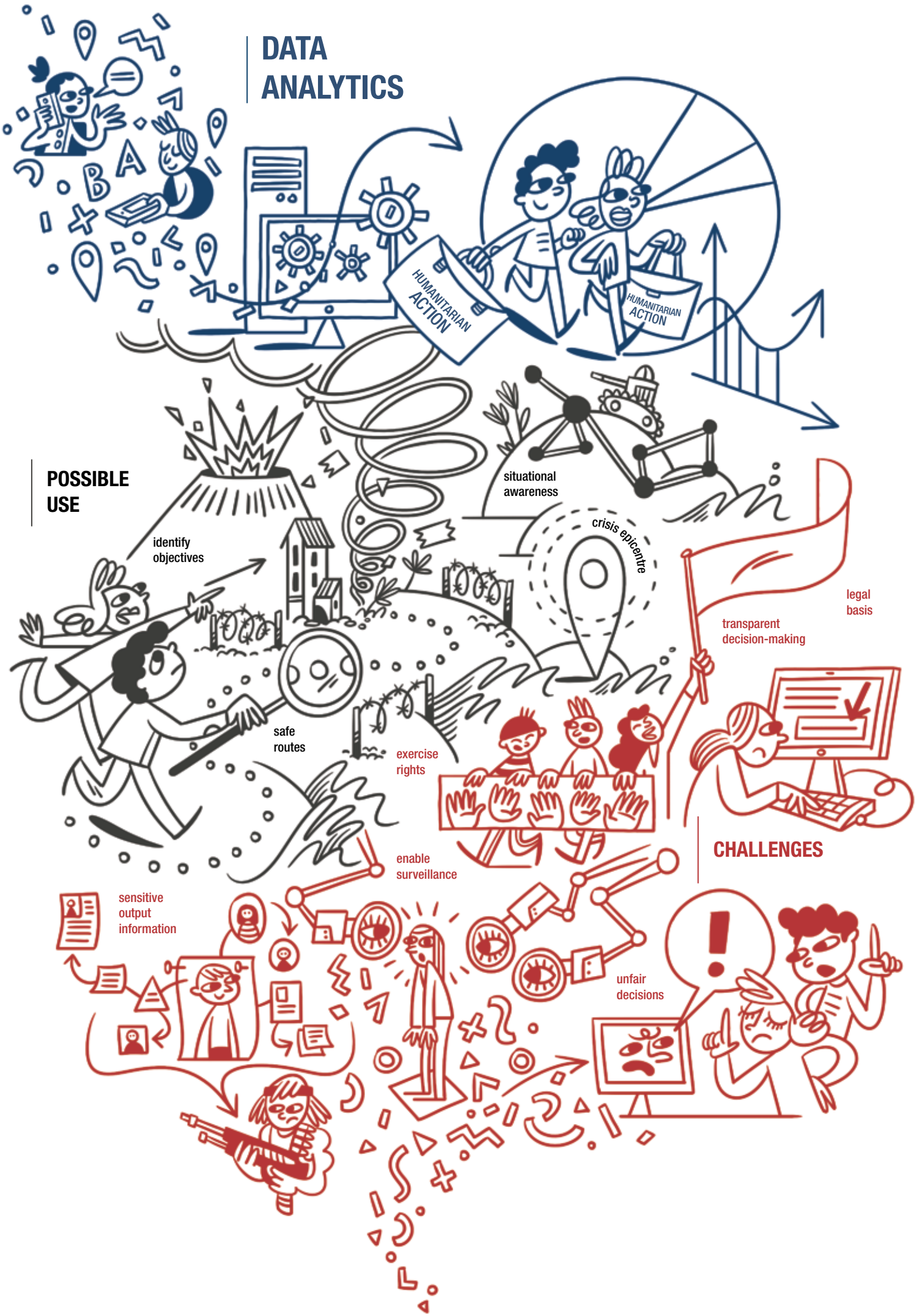
In addition to documenting and implementing data protection decisions, a Humanitarian Organization should consider whether it would be useful to Data Subjects or to the public to understand the considerations underlying its data protection decision-making. Accordingly, the organization might then share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

5.2.10 Provide expert review and/or audit of the DPIA

Humanitarian Organizations should ensure that a data protection expert, such as the organization's Data Protection Officer or his/her staff, reviews or audits the implementation of the DPIA.

5.2.11 Update the DPIA if there are changes in the project

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


DATA ANALYTICS
HUMANITARIAN ACTION
HUMANITARIAN ACTION
POSSIBLE USE
identify objectives
situational awareness
crisis epicentre
safe routes
exercise rights
legal basis
transparent decision-making
CHALLENGES
enable surveillance
sensitive output information
unfair decisions

Chapter 6:
DATA ANALYTICS AND BIG DATA

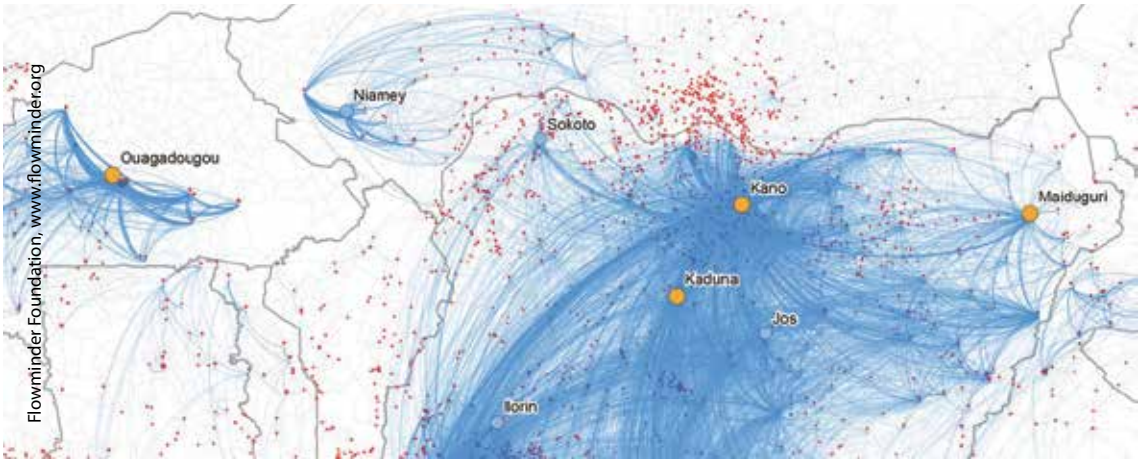
6.1 Introduction

As Humanitarian Action is driven by information;[76] performing Data Analytics through Personal Data Processing has potentially significant benefits for Humanitarian Organizations. The term "Data Analytics" denotes the practice of combining very large volumes of diversely-sourced information (Big Data) and analysing them, using sophisticated algorithms to make informed decisions. Big Data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on the possibility of analysing, understanding and taking advantage of the full value of data (in particular using Data Analytics applications). For the purposes of this chapter the two terms, "Data Analytics" and "Big Data", will be used interchangeably.

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

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

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



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

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

The use of Data Analytics has often given rise to accusations of misleading and inaccurate results; justifying arbitrary and automated decisions that do not take case-specific particularities into consideration; generating data that may

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

be used to enable more effective surveillance through digital footprints; and the possibility of breaching anonymity through reverse engineering, therefore leading to re-identification of individuals included in the Processing. The data protection implications of Big Data were highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Big Data, adopted in Mauritius in 2014.[77]

Concerns may also be raised when applying basic data protection principles to Data Analytics, for instance with regard to 1) purpose specification insofar as Data Analytics Processing uses Personal Data for previously unforeseen purposes; 2) transparency requirements, given that not much information is typically provided to Data Subjects; or 3) the principle of legitimate Processing, which is not always easily identifiable as a suitable legal basis for the Processing.[78]

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

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

- *Data sources*. First of all, it is important to identify the source of data. Much Data Analytics Processing undertaken by Humanitarian Organizations is based on publicly available data, such as information from government agencies or public records, social media networks, census data and other publicly available demographic and population surveys. In other cases, Humanitarian Organizations may partner with private enterprises such as telecommunications or infrastructure companies, internet services, healthcare providers or other commercial organizations to improve the humanitarian and disaster response.
- *Emergency response*. Although the outputs from Data Analytics have irrefutable benefits for Humanitarian Organizations, they may not always be used for an ongoing emergency or to address the vital interests of the individuals concerned. There may, for example, be cases where Data Analytics Processing takes place after an incident has occurred and has been dealt with, to support administrative work or to contribute to strategies to improve the response to future emergencies.
- *Accuracy*. Data used for analytics may not always be representative and accurate and may contain bias, which can lead to incorrect results.[79] Working on anonymized or aggregated data, while potentially less intrusive vis-à-vis the privacy of the individuals involved, may increase this risk.
- *Automated decision.* Data Analytics with no human intervention or contextual background can also lead to incorrect insights and decisions.[80]
- *Reuse of data for other purposes*. The use of Big Data often poses questions about whether Personal Data can be used for purposes other than those for which they were collected. This raises questions under data protection law, which generally requires that Personal Data be collected for defined purposes and processed for such purposes or for compatible purposes only, and not reused for other purposes without the Consent of the individual concerned or some other legal basis.
- *The sensitivity of data output created by Personal Data Processing in humanitarian situations*. It is important to understand that otherwise publicly available data, for instance data on social media networks and

77 International Conference of Data Protection and Privacy Commissioners, Resolution on Big Data, Fort Balaclava, Mauritius, 2014: https://icdppc.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf.

78 See Chapter 2: Basic principles of data protection.

79 UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report, page 12: http://unglobalpulse.org/sites/default/files/Big_Data_for_Development_and_Humanitarian_Action_Report_Final_0.pdf.

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

data not generally considered as sensitive, may generate Sensitive Data when processed for Data Analytics purposes in a humanitarian situation. This can happen when Processing anodyne data enables the profiling of individuals which could result in discrimination or repression, such as, for example, potential victims, people affiliated with a particular group in a situation of violence, or bearers of a particular illness. In these cases, *data smoothing* can be a valuable way to protect individual and group privacy while allowing access to data.[81] However, it is important to note that as data are temporally and spatially *smoothed*, the clarity of findings is also diminished.

- *Anonymization*. Doubts may exist as to the effectiveness of Personal Data Anonymization and the possibility of re-identification in Data Analytics operations, regardless of whether for humanitarian or other purposes. Again, data smoothing can complement Anonymization to provide another layer of protection to prevent re-identification.
- *Regulatory fragmentation*. While many states have enacted data protection law and many Humanitarian Organizations have already implemented data protection policies and guidelines, the question of how specifically Big Data are regulated across borders at times of humanitarian crises remains open.[82]

It is important to realize that when Data Analytics are used for Humanitarian Action, the implications for individuals may be far more serious than in other settings (e.g. Data Analytics performed in a commercial environment). For example, even when the analysed data have been anonymized, the results may have severely negative consequences not only for individuals but also for groups of individuals. Humanitarian Organizations should consider whether any data they release or conclusions they draw from Data Analytics may be used, even in the aggregate, to target the people they seek to protect. Furthermore, such potentially affected groups of individuals do not always include the Data Subjects. In many cases invisible populations can suddenly become visible by being separated from the group identified by the data set.[83] It is important, therefore, always to keep in mind the "big picture" of the potential implications of Data Analytics on vulnerable individuals.

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

Data Analytics may involve Processing scenarios such as the following:

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

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

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

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

81 Data smoothing means to remove noise from a data set so that important patterns stand out.
82 UN Global Pulse, *Big Data for Development and Humanitarian Action: Towards Responsible Governance*, Privacy Advisory Group Report, pages 7-9, *op. cit.*
83 ibid, page 12.

The following data sets may be relevant:

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

Humanitarian Organizations may play the following roles in data Processing:

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

These scenarios can be presented as follows:

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

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

6.2 Application of basic data protection principles

Processing Personal Data for Data Analytics presents important challenges for individual data protection. When the Processing uses large data sets that are processed for purposes other than those for which they were collected, it risks violating basic notions of data protection, including purpose limitation, data minimization or the retention of data for only as long as necessary for execution of the purposes of collection. In essence, Data Analytics thrive in open

and unrestricted Processing environments while, on the other hand, Personal Data protection favours limited and well-defined Personal Data Processing. It is for this reason that data protection needs to be applied innovatively to Data Analytics.[84]

The basic principles of data protection constitute the baseline to be respected while engaging in Data Analytics Processing. As mentioned in Chapter 2: Basic principles of data protection, the basic data protection principles that need to be respected while undertaking Data Analytics include the principle of the fairness and lawfulness of the Processing; the principle of transparency; the purpose limitation principle; the data minimization principle; and the data quality principle. While some of these principles are compatible with the purposes of Data Analytics, others may raise questions or conflicts, and consequently special care must be taken by Humanitarian Organizations when applying them in practice. Other Humanitarian Organizations have developed principles for handling Big Data that complement the discussion in the present Chapter.[85]

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

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

6.2.1 Purpose limitation and Further Processing

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

With regard to Further Processing, irrespective of the legal basis used for the initial Processing, Humanitarian Organizations may process Personal Data for purposes other than those initially specified at the time of collection where the Further Processing is compatible with those purposes, including where the Processing is necessary for historical, statistical or scientific purposes.[86]

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

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

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

86 See Section 2.6.3 Further Processing.

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

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

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

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

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

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

6.2.2 Legal bases for Personal Data Processing

If the purposes of analytics are deemed to be incompatible with the original purpose of Processing, a new legal basis for the analytics should be found. In using Data Analytics, Humanitarian Organizations could process Personal Data based on one or more of the following:[87]

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

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

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

In order to ensure Consent is properly informed, the information provided should take into account the outcome of the DPIA[88] and might also be given via an interface which simulates the effects of the use of data and its potential impact on the Data Subject, in a learn-from-experience approach.[89] Data Processors should provide easy and user-friendly technical ways for Data Subjects to withdraw their Consent and to react to data Processing incompatible with the initial purposes.[90]

It is important to assess the validity of Consent even when adequate information has been provided to the Data Subjects at the time of collection and the purpose of Further Processing is compatible. This assessment should take into account the Data Subject's level of literacy as well as the risks and harms to the Data Subjects for the Processing of their data.[91]

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

87 See Chapter 3: Legal bases for Personal Data Processing.
88 See Section 6.7 Data Protection Impact Assessments.
89 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Guidelines on the protection of individuals with regard to the processing of the personal data in a world of Big Data*, January 2017, *op. cit.*
90 *ibid*.
91 United Nations Development Programme (UNDP), UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*: http://www.unglobalpulse.org/privacy/tools.

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

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

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

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

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

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

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

6.2.3 Fair and lawful Processing

To be fair and lawful the Processing requires a legal basis, as detailed in Section 2.5 Data Processing principles.

Data Analytics deals in possible correlations, rather than objectivity, and therefore raises numerous questions about the fairness of the Processing, including concerns about sampling, representation and population estimates. Researchers should take care to understand the representativeness of the sample data, attempt to use broad and representative data sets, and report potential biases.

Moreover, policymakers should account for these biases when making decisions. When used in policy making, basing analytics on inaccurate data and misinterpretations of findings could lead to harmful and/or unfair policy decisions, or Data Subjects may find themselves affected by potentially biased automated decisions and by generalizations.

In addition, the fairness requirement in data protection law is generally focused on the provision of information, transparency and the impact of the Processing. In Data Analytics, given the complexity of the Processing and the difficulty in performing a meaningful risk analysis, transparency about methodology (including where possible the algorithm) is very important, so that the rigour of the approach can be independently assessed, above and beyond the Data Subjects' right of information.[92] Care should be taken in decision-making processes about transparency if transparency conflicts with data sensitivity at the individual level, or when transparency in Processing could encourage gamification of the data Processing system by malicious actors and therefore bias it.

The principle of fairness implies that an assessment of the risks of re-identification should be carried out before de-identification and, where possible, the Data Subject or relevant stakeholders be informed of the results of the assessment. If there is a strong possibility of re-identification, a decision should be taken not to perform the analytics or to adjust the methodology. The proper assessment of such a Data Analytics situation requires the performance of a DPIA.[93]

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

6.2.4 Data minimization

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

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

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

92 See Section 6.3 Rights of Data Subjects and Section 6.5 International Data Sharing.
93 See Section 6.7 Data Protection Impact Assessments.

should therefore be carefully selected to minimize the risks of re-identification and ensure that the data remain of the right quality and utility to achieve credible results.

Data Controllers and, where applicable, Data Processors should carefully consider the design of their data analysis, in order to minimize the presence of redundant and marginal data.[94]

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

If this Processing is performed on pre-existing data sets, as "compatible Further Processing",[95] the Processing should take place within the data retention period allowed for the purpose of initial collection. Renewal of the initial retention period, if a renewal is contemplated by the retention policy at the time of collection, can take place to enable analytics as "compatible Further Processing".

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

6.2.5 Data security

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

In this case, the Humanitarian Organization undertaking the Data Analytics should implement adequate security measures to protect the output, which are appropriate for the risks involved.[96] Additionally, regular data security and data privacy training is essential to raise awareness of security threats and to avoid data breaches.

6.3 Rights of Data Subjects

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

The Data Subject's exercise of the right to information (also relevant to the transparency principle, see Section 6.2.1 Purpose limitation and Further Processing) is more difficult with Data Analytics, as it is not always possible to provide detailed information on the Processing directly to the individuals

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

95 See Section 2.6.3 Further Processing.

96 See Section 6.2.5 Data security and Section 2.8 Data security and Processing security.

concerned, particularly when Processing takes place on existing data sets. It is therefore important to explore alternative means of information provision, for example, by using the websites of the organizations involved, other internet platforms likely to be used by the Data Subjects, or other means of mass communication (e.g. newspapers, leaflets or posters). Where the provision of information to Data Subjects proves difficult or impossible, the creation of a national or cross-national information resource (easier to be found than websites of single operators) has been suggested. It may also be advisable to investigate providing information to group representatives.

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

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

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

6.4 Data sharing

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

6.5 International Data Sharing

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

- Humanitarian Organizations employing Data Processors, i.e. commercial entities, undertake the actual Processing of Personal Data on the data held by the Humanitarian Organization.
- Humanitarian Organizations asking commercial entities that are and remain the Data Controller of the data to carry out analytics on such data for humanitarian purposes, and provide conclusions/findings to the Humanitarian Organization. Such conclusions could involve either aggregated/anonymized data, or data identifying individuals of possible relevance for Humanitarian Action.

- Sharing data sets among Humanitarian Organizations, public authorities and/or commercial entities (joint Data Controllers and/or Data Processors).
- Actual sharing (or transferring data) to a Humanitarian Organization for Processing by it.

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Data Analytics are conducted, as discussed above.[97] It is essential to perform a DPIA[98] prior to International Data Sharing for Data Analytics, given the complexity of Data Analytics, the difficulties in ensuring that Data Subjects are adequately informed and are in a position to fully exercise their rights as mentioned above, and the potentially far-reaching implications of Data Analytics for them. Indeed, a DPIA will be the most suitable tool to identify the possible risks involved in data sharing, and the most suitable mitigating measures available (e.g. contractual clauses, codes of conduct, or indeed refraining from data sharing).[99]

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

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

6.6 Data Controller/Data Processor relationship

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

97 See Section 6.2.2 Legal bases for Personal Data Processing.
98 See Section 6.7 Data Protection Impact Assessments.
99 See Chapter 4: International Data Sharing and Section 4.4 Mitigating the risks to the individual.

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

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

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

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

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

6.7 Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of applicable data protection regulations and potential risks are covered.[100] DPIAs are now required in many jurisdictions and by some Humanitarian Organizations. However, it can be more difficult to implement them with regard to new technologies, where risks are less clear. Apart from clarifying the details and specifications of the Processing, DPIAs should focus on the risks posed by it and on mitigating measures.

Accordingly, DPIAs need to be conducted prior to any Data Analytics operations. Of particular significance are risk assessment tools that have been specifically developed to assess the risks of Data Analytics in Humanitarian Action, such as the UN Global Pulse Data Innovation Risk Assessment Tool.[101]

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

- re-identification of individuals of relevance for Humanitarian Action, when the purpose of analytics is to identify patterns;
- risks for the viability and security of humanitarian operations, in cases where data of alleged perpetrators of violations of international humanitarian or human rights law are processed;
- risks that if a Humanitarian Organization makes requests about specific patterns or categories of individuals of interest to authorities or corporations, this may lead to such Third Parties discriminating or otherwise taking an interest in them with detrimental implications for them and for the neutrality of Humanitarian Action;

100 See Chapter 5: Data Protection Impact Assessments (DPIAs).
101 United Nations Development Programme (UNDP), UN Global Pulse, *Tools, Risks, Harms and Benefits Assessment*: http://www.unglobalpulse.org/privacy/tools.

- risks that the results of the Data Analytics operation performed by Humanitarian Organizations to which a Third Party gains access may be exploited by commercial Third Parties and/or authorities for unrelated purposes;
- risk that Data Analytics outputs may be accessed and used by parties in a situation of violence or conflict to gain an advantage vis-à-vis other stakeholders and thus compromise the safety of the Data Subjects and the neutrality of Humanitarian Action;
- risk that commercial providers who perform analytics on their own data or who process Humanitarian Organizations' data may have incentives to exploit the findings of the Processing for commercial purposes to improve their understanding of their current or potential customers or for further customer profiling.[102]

DPIAs for Data Analytics also take into account the likelihood, magnitude and severity of the harm that could result from the risks. Such risks and harm should then be assessed against the likely expected benefits from Data Analytics and taking into account the principle of proportionality.[103]

Specific risk-mitigating measures may include:

- Anonymization as a technical measure; and
- legal and contractual obligations to prevent possible re-identification of the persons concerned.[104]

102 See Section 2.3 Aggregate, Pseudonymized and Anonymized data sets.

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

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

DRONES


POSSIBLE USE
search and rescue operations
mapping emergency situations
complement traditional assistance
monitoring the spread of disease
CHALLENGES
issues of transparency
sensitive information
crowdsourcing to process and analyse big data
legitimate processing and exercise of rights

Chapter 7:
DRONES/UAVS AND REMOTE SENSING

7.1 Introduction

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

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

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

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

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

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

In disaster situations "drones may be used to provide relief workers with better situational awareness, as they can locate survivors amidst the rubble, perform structural analysis of damaged infrastructure, deliver needed supplies and equipment, evacuate casualties, and help extinguish fires – among many other potential applications."[105] Drones can also supply aerial data from areas which

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

are considered unsafe for Humanitarian Action providers (e.g. sites contaminated by radioactivity or wildfire locations).[106]

Nevertheless, while Drones may be an invaluable source of direct and indirect information when responding to emergencies, a critical assessment has to be made before they are used in any particular case. Their use may include significant risks.[107] Apart from safety issues *per se* (e.g. accidents during their deployment that could result in bodily injury or even death), they may be perceived as spying or intruding in a conflict scenario, something that could severely compromise the safety of their operators and the staff of Humanitarian Organizations, as well jeopardizing local people who may be perceived by the parties in the conflict as having given Consent to the use of Drones on their behalf.

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

It is worth noting that concerns about potential violations of Personal Data protection rights are not caused by the use of Drones, but rather by the on-board equipment which can process Personal Data. Information technologies embedded in Drones or connected to them can perform various data Processing activities and operations (e.g. data collection, recording, organization, storage and combination of collected data sets). Data typically collected by drones include video recordings, "images (e.g. images of individuals, houses, vehicles, driving license plates, etc.), sound, geolocation data or any other electromagnetic signals related to an identified or identifiable natural person."[108] Depending on the quality of the data, it may be possible to identify individuals directly or indirectly. This can be done either by a human operator or automatically, for instance by capturing an image from a facial recognition programme/algorithm, scanning to detect a smartphone and using it to identify the person or using radio-frequency identification (RFID) chips in passports.[109]

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

- It is technically possible to make aerial Drones flight-specific, on the basis of unique identifiers embedded in their basic equipment.
- Permission to fly Drones and a remote pilot's licence issued by the state authorities are required in many countries.[110]
- Imagery data (of various levels of analysis and quality) are the most common type of data collected by Drones.
- Altitude of flight and angle of capture of the imagery also have a significant impact on the likelihood that the imagery captured may directly or indirectly identify an individual.
- Although technology is advancing rapidly, at present Drones can capture extremely detailed pictures, but most cannot capture individuals' faces.

106 American Red Cross, et. al., *Drones for Disaster Response and Relief Operations,* April 2015, page 4: http://www.issuelab.org/resources/21683/21683.pdf.
107 Delafoi F, *Le drone, l'allié ambigu des humanitaires*, Le Temps, 11 April 2016: https://www.letemps.ch/monde/2016/04/11/drone-allie-ambigu-humanitaires; *What do Tanzanians Think About Drones? Now We know*, ICT Works, 22 February 2016: http://www.ictworks.org/2016/02/22/what-do-tanzanians-think-about-drones-now-we-know/.
108 Article 29 Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, page 7: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.
109 *ibid*., page 14.
110 Storyhunter Guide to Commercial Drone Regulations Around the World: https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world.

The picture has to be connected to other data sets in order to lead to identification. When facial identification is not possible, identification may be possible through the use of location and other types of data. The use of metadata (data that provides information about other data) is crucial in this context.

- It is important to establish where data collected are kept and what types of Processing are performed on them; in this respect there is a correlation between Drones and the use of Data Analytics.[111]
- A number of international initiatives on standards and other drone-use specifications are currently under way, some looking specifically at the use of Drones for humanitarian purposes. Humanitarian Organizations are advised to follow these initiatives closely and apply their findings in their practices.[112]
- Humanitarian Organizations often outsource the drone operations to professionals, which therefore raises data protection issues (e.g. Data Controller/Data Processor relationship, access to data, etc.).
- Drone-related Personal Data Processing often involves cross-border transfers, which require a legal basis under data protection law.

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

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

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

7.2 Application of basic data protection principles

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

7.2.1 Legal bases for Personal Data Processing

Humanitarian Organizations can process Personal Data collected by Drones using one or more of the following legal bases:[113]

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

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

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

111 See Chapter 6: Data Analytics and Big Data.
112 See for example, *Humanitarian UAV Code of Conduct & Guidelines*: http://uaviators.org/docs.
113 See Chapter 3: Legal bases for Personal Data Processing.

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

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

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

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

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

As has already been mentioned in Chapter 3: Legal bases for Personal Data Processing, given the nature of Humanitarian Organizations' work and the emergency situations in which they operate, in some circumstances there may be a presumption that the Processing of data necessary for humanitarian purposes is in the vital interest of a Data Subject.[114]

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

EXAMPLES:

- The use of Drones in search and rescue operations by a Humanitarian Organization would most likely qualify under this legal basis, because it would protect the vital interest of the Data Subject (i.e. the person unaccounted for).
- The use of Drones in mapping operations by a Humanitarian Organization, in the absence of a specific emergency, would most likely not qualify under this legal basis, because there is no direct connection with the vital interests of the Data Subjects living or moving around in the areas being mapped.

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

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

EXAMPLE:

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

7.2.2 Transparency/Information

The principle of transparency requires that at least a minimum amount of information concerning the Processing be provided to the Data Subject. In addition, information and communications about the Processing should be easily accessible and easy to understand, express in clear and plain language. For obvious

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

practical reasons these requirements can be difficult to satisfy in the case of Drones. Timing of information is also important; in non-emergency situations, this should ideally take place in advance of and during Drone flights. The involvement of community leaders and authorities or media campaigns targeted at the envisaged Data Subjects (e.g. radio, newspapers and posters in public areas) can help fulfil transparency obligations.

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

7.2.3 Purpose limitation and Further Processing

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

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

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

7.2.4 Data minimization

Personal Data may only be processed if adequate, relevant and not excessive in relation to the purposes for which they were collected. Therefore, a strict assessment of the necessity and proportionality of the processed data should take place.[115] Moreover, when Drones are used for humanitarian purposes, the principle of data minimization should be respected by choosing proportionate technology and by adopting measures of data protection and privacy by design and by default.

115 See Chapter 2: Basic principles of data protection.

For instance, Humanitarian Organizations could consider the following options:

- privacy settings on services and products should by default avoid the collection and/or the Further Processing of unnecessary Personal Data;
- implementation of Anonymization techniques;
- automated blurring of faces/human beings (or only certain particular categories of more vulnerable individuals); and
- increased flight altitude, or angle of capture of imagery to minimize the likelihood of capturing imagery that can directly identify individuals.

7.2.5 Data retention

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

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

7.2.6 Data security

A Humanitarian Organization deploying Drones should implement adequate security measures that are appropriate for the risks involved.[116] For Drones, this could include encryption of databases or temporary storage devices on board, as well as end-to-end encryption of data in transit between the drone and the base, where applicable.

7.3 Rights of Data Subjects

The rights of the Data Subject have already been described in Chapter 2: Basic principles of data protection. The following are some further remarks about Data Subjects' rights with respect to Humanitarian Organizations' use of Drones.[117]

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

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

In practice, however, it could prove challenging for Humanitarian Organizations to provide Data Subjects with information along the above lines when using Drones to collect Personal Data. Nonetheless, the various options to be decided on a case by case basis could include: information campaigns, public notices and other similar measures. Drone operators should publish information on their website or on dedicated platforms to inform individuals about the

116 See Chapter 2: Basic principles of data protection.
117 See Section 2.11 Rights of Data Subjects.

different operations that have taken place as well as forthcoming ones. In remote areas or where it is unlikely that individuals can access the internet, information can be published in newspapers, leaflets or posters, or provided by means of a letter or radio broadcast.

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

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

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

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

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

7.4 Data sharing

The circumstances under which personal information is exchanged between Humanitarian Organizations or between Humanitarian Organizations and Third Parties need to be identified and addressed with respect to data protection. Information collected by Drones may be shared either at the moment of collection or at a later stage. Humanitarian Organizations may outsource drone-related work to Data Processors. In the event that any of the above involves Personal Data being shared across national borders, the relevant issues concerning International Data Sharing also need to be addressed.[118]

118 See Chapter 4: International Data Sharing.

In these cases, it is important to consider the following:

- The data protection roles of the Humanitarian Organizations concerned.[119]
- Whether imagery or other information exchanged should include Personal Data or whether it is sufficient to share only the conclusions and findings of the analysis and assessment of the imagery collected (no raw data exchange).
- Involuntary or accidental data sharing (e.g. if imagery is saved on the device and the device is captured), or if an aerial imagery feed is transmitted in a non-secure and unencrypted way. The impact of this should also be taken into consideration by the Humanitarian Organizations involved.

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

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

7.5 International Data Sharing

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Drones are used, as discussed in Chapter 4: International Data Sharing. Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and in line with their own internal policies before carrying it out. Performing a DPIA prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing.[120]

7.6 Data Controller/Data Processor relationship

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

119 See Section 7.6 Data Controller/Data Processor relationship.
120 See Section 7.7 Data Protection Impact Assessments.

EXAMPLES:

- A Humanitarian Organization whose own staff operate Drones for its own purposes is the (only) Data Controller for such Processing.
- A Humanitarian Organization outsourcing a Drone operation to a specialized corporation, whose sole task is to pilot the Drones, would be the (only) Data Controller for such Processing; the corporation would be the Data Processor for this operation.
- Two Humanitarian Organizations who wish to use Drones and outsource all relevant operational work to a corporation having no access to the data collected will be joint Data Controllers. The corporation would be the Data Processor for the operation.

7.7 Data Protection Impact Assessments

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

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

BIOMETRICS


sensitivity level
POSSIBLE USE
uniquely identifies individuals without other means of proving who they are
efficiently identifies individuals
CHALLENGES
data minimization
reliability of data
technical difficulties
irreversible
difficulties with consent
humanitarian purpose ethical issues

Chapter 8:
BIOMETRICS

8.1 Introduction

The International Organization for Standardization defines biometric recognition and Biometrics as the "automated recognition of individuals based on their biological and behavioural characteristics".[121] Biometrics are therefore measurable, unique human signatures that may include fingerprints, iris scans or behavioural characteristics such as the way a person walks.

The data protection implications of the use of biometric data, with particular reference to the use of biometric data in passports, identity cards and travel documents, have been highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Biometrics, adopted in Montreux, Switzerland, in 2005.[122]

Humanitarian Organizations around the world increasingly deploy biometric recognition as part of their identification systems because of the benefits it can bring in efficiently identifying individuals and preventing fraud and/or misuse of humanitarian aid. Indeed, paper-based identification mechanisms (identity cards, ration cards, wrist bands, etc.) that constitute the non-digital alternative have limitations, as they may easily be lost or counterfeited, require substantial resources to crosscheck (thereby giving rise to potential duplication and inefficiency), and in most cases do not allow for automated Processing. In certain situations, it is suggested that these shortcomings may be overcome through the use of biometric identification systems (often as an additional means of verification). Biometric data are more difficult to counterfeit and, being digitally produced and stored, facilitate the efficient management of humanitarian aid in the field and can also be used for Data Analytics or other types of advanced data Processing operations. In addition, by focusing on the individual's unique features, Biometrics can confirm the identity of individuals who have no other means of adequately proving it, which is often the case with displaced people, and therefore put individual identity and dignity at the heart of Humanitarian Action.[123]

However, these promises have not always been fulfilled in the actual deployment of Biometrics identification systems. Some projects to implement Biometrics have reportedly faced considerable problems with regard to the reliability of the relevant systems.[124] Inherent limitations, such as the fact that individuals' fingerprints are not always readable, provide further difficulties in implementation. Ethical issues may also arise, for example, by virtue of the use of biometric data in national identification systems and the problematic legacies of such systems in certain countries.[125] Additionally, due to the interest in biometric data for national law enforcement and national security purposes, Humanitarian Organizations may find themselves under increasing pressure to share data with national and regional authorities for purposes which go beyond humanitarian work. Interest in biometric data means that it faces a significant risk of unauthorized access by Third Parties i.e. hacking.

Humanitarian Organizations may use biometric technologies for Processing operations such as the collection and management of data on displaced persons who have to be registered for the purposes of humanitarian aid distribution, including Cash Transfer Programmes.[126]

121 See ISO/IEC 2382-37:2017 Information technology - Vocabulary - Part 37: Biometrics: https://www.iso.org/standard/66693.html.
122 International Conference of Data Protection and Privacy Commissioners, Resolution on Use of Biometrics in passports, identity cards and travel documents, Montreux, Switzerland, 2005: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Biometrics-in-passports-identity-cards-and-travel-documents.pdf.
123 See for example, Hugo Slim, *Eye Scan Therefore I am: The Individualization of Humanitarian Aid*, European University Institute Blog, 2015: https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/; Paul Currion, *Eyes Wide Shut: The challenge of humanitarian biometrics,* IRIN, 2015: http://www.irinnews.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics.
124 Gus Hosein and Carly Nyst, *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, IDRC/UKaid, 2014, page 16.
125 *Ibid.*, page 19.
126 See Chapter 9: Cash transfer programming.

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

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

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

- accurate individual identification;
- combatting fraud and corruption;
- increased donor support and credibility of programming (as a consequence of the points above);
- greater efficiency through the digital Processing of identification data;
- greater efficiency in the physical protection of individuals/minimization of the risk of disappearance;
- putting individual identity and dignity at the heart of Humanitarian Action;
- enhancing the right of individuals to move freely;
- enhancing the resettlement of individuals into third countries; and
- enabling bank account acquisition.

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

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

8.2 Application of basic data protection principles

The use of biometric technologies raises significant data protection issues. Biometric information is considered to be Personal Data and therefore covered by data protection legislation. For example, the EU General Data Protection Regulation expressly regulates biometric data, defining them as "Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[127] In many legal systems, biometric information is considered to be "Sensitive Data."[128] Consequently, special, detailed requirements apply to the Processing of this type of data, directly affecting the lawfulness of the Processing in the event that they are not met.

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

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

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

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

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

When undertaking DPIAs, Humanitarian Organizations should take into account the fact that different types of biometric data may have different levels of "sensitivity". Some categories of biometric data, while sensitive for the reasons set out above, may be more or less sensitive than others. Fingerprints, for example, may be depleted or erased, whether unintentionally (e.g. through heavy manual work), or intentionally, thus making this type of data less sensitive than others. On the other hand, iris scans may potentially enable the extraction of very sensitive information beyond the identification of the individual. Furthermore, certain types of biometric data may only be collected and read with the direct participation of a Data Subject, such as palm vein recognition, thus making this type of data less sensitive than others. Other categories of biometric data, such as iris information, can be read from a distance, thus making it particularly sensitive.[129]

Consequently, even when the legislation governing Personal Data Processing mentioned above does not apply, Processing biometric data presents special risks and requires an increased level of care. Processing should therefore be subject to a careful preliminary review, in order to establish whether certain safeguards (for example, increased security measures) need to be in place before, during and after its execution, as discussed further below, or if biometric data should be used at all, considering the potential risks involved.

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

8.2.1 Legal bases for Personal Data Processing

Humanitarian Organizations may process Personal Data using one or more of the following legal bases:[130]

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

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

130 See Chapter 3: Legal bases for Personal Data Processing.

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

- the individuals' physical inability to provide it, such as in cases of unconscious patients (where, for example, biometric data may be required to unlock a patient medical file, combined with other legitimate authority to unlock);
- the shortage of time and staff to ensure adequate counselling during the first phases of an emergency, when the priority is to provide lifesaving assistance;
- the individuals' vulnerability and/or legal inability to provide it;
- the highly technical nature and irreversible nature of the data potentially exposing individuals to risks that are difficult to understand or contemplate when Consent is given. This refers particularly to the possibility that science and technology may develop in ways that pose new risks not foreseen at the time of Consent (e.g. genetic information becoming accessible from a scan of an individual's iris); and
- no real choice is provided as to alternative ways of receiving assistance or protection (for example, if you are dependent on humanitarian aid for you survival or that of your family, or if you need to register to remain legally in the country in which you are located, there is very limited opportunity for you to refuse the collection of your biometric data).

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

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

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

It could be argued that in difficult conditions, because of the effectiveness of Biometrics to identify individuals, the vital interests of the Data Subject or another person might constitute a plausible alternative legal basis for the relevant Processing in cases when Humanitarian Organizations are unable to obtain the individuals' Consent. Furthermore, it is possible to imagine a situation in which the use of biometric systems can be argued to be justified by the promotion of the beneficiaries' vital interests. For example, if only limited resources are available for Humanitarian Action and some potential beneficiaries do not receive essential assistance because aid is fraudulently overprovisioned to another group of individuals, biometric systems can facilitate accurate resource allocation and fraud prevention. On the other hand, it can also be argued that biometric data are not essential for the purposes of distributing aid. The use of biometric data responds more to the Humanitarian Organizations' need to carry out their work in an efficient and effective manner, avoiding the risk of duplication and the waste of financial resources, rather than responding to the vital interests of the individuals concerned.

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

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

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

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

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. Such legitimate interests may include Processing necessary to increase the efficiency of the delivery of humanitarian assistance, reduce costs and risks of duplication and fraud. However, considering that biometric data can be used for potentially intrusive purposes and given their specific features highlighted above, it can be questioned whether the rights and freedoms of a Data Subject do not always override the legitimate interests set out above. Before the legitimate interests of the Data Controller can be used as a legal basis, a careful analysis of the risks and of possible interference with the fundamental rights and freedoms of the Data Subject would have to be included in the relevant DPIA. This is particularly important in cases where a risk may be envisaged that Third Parties could gain unauthorized access to the data, or put pressure on Humanitarian Organizations to provide this highly Sensitive Data and use them for other than exclusively humanitarian purposes.

8.2.2 Fair and lawful Processing

Under data protection law, Personal Data need to be processed lawfully and fairly.[131] Lawfulness of the Processing refers to the identification of an appropriate legal basis. The requirement for fairness is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations involved in biometric data Processing should keep in mind that these principles need to be applied during all stages of Processing.

8.2.3 Purpose limitation and Further Processing

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

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

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

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

131 See Section 2.5.1 The principle of the fairness and lawfulness of Processing and Section 8.2.2 Fair and lawful Processing.

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

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

As explained above,[132] purposes within the wider category of "humanitarian purposes" are likely to be compatible with Further Processing operations. This would, however, not be the case if new risks are involved, or if the risks for the individuals concerned outweigh the benefits of Further Processing. This assessment would depend on the circumstances of the case, and include an analysis of any risks that Processing may be against significant interests of the person to whom the information relates or his/her family, in particular, when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or reputation.

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

8.2.4 Data minimization

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

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

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

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

132 See Section 8.2.3 Purpose limitation and Further Processing.

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

8.2.5 Data retention

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

8.2.6 Data security

Given the sensitive nature of biometric information as well as its potential misuse if unauthorized access is granted to it or otherwise obtained,[133] it is imperative that adequate, proportionate security measures are implemented by the Humanitarian Organization determining the purposes and means of the Processing (i.e. by the Data Controller). For example, encryption or compartmentalization of information could constitute viable solutions to this end for Humanitarian Organizations.

8.3 Rights of Data Subjects

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

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

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

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

8.4 Data sharing

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

- The Humanitarian Organization hires an external Data Processor to provide the Biometrics technology required to collect and process the data. In this case a Data Controller/Data Processor relationship is established.
- The Humanitarian Organization carries out a transfer of data to a Third Party, which becomes a new Data Controller.
- The authorities of the host country request or require a copy of biometric data collected on their territory, either in bulk or for specific individuals.

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

8.5 International Data Sharing

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

Data protection law restricts International Data Sharing and Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Biometrics are used, as discussed above.[134] Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out. Performing a DPIA[135] prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing from a data protection perspective.

8.6 Data Controller/Data Processor relationship

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

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

134 See Section 8.2.1 Legal bases for Personal Data Processing.
135 See Section 8.7 Data Protection Impact Assessments.

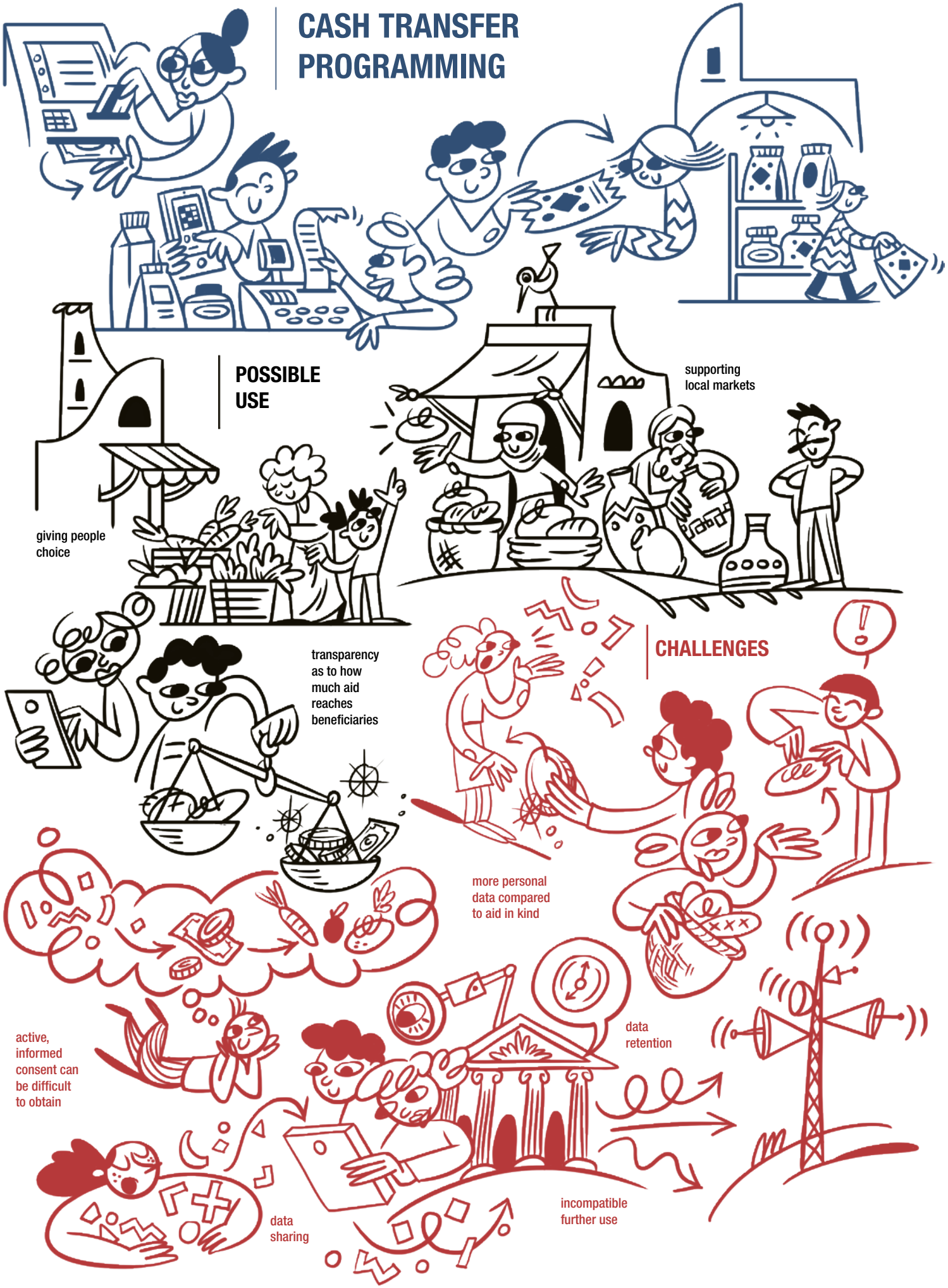
segregated should be carefully assessed. DPIAs, drafted prior to the Processing of Biometrics data, may be a suitable means of clarifying the roles of different parties engaged in the Processing.

8.7 Data Protection Impact Assessments

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

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

CASH TRANSFER PROGRAMMING



Chapter 9:
CASH TRANSFER PROGRAMMES

9.1 Introduction

Cash transfer programming is a promising tool for supporting processes of survival and recovery from Humanitarian Emergencies. The terms Cash Transfer Programme, cash transfer programming or cash assistance intervention can be used interchangeably and are understood to encapsulate all types of cash transfer programmes, i.e. both vouchers and cash, and all types of delivery mechanisms. Some organizations also refer to cash-based assistance, which is an equivalent term.[136]

In practice, these terms often refer to cash transfers or electronic vouchers that can be spent on pre-designated products in specific shops. These cash transfers maximize the respect for beneficiaries' choices and the trade-offs they face. The world of humanitarian response continues to experiment with several different varieties of cash assistance, ranging from vouchers that have to be exchanged for specific products, to cash transfers that are made conditional on beneficiaries meeting some kind of requirement, to unrestricted and unconditional cash transfers.[137]

There are different forms of electronic cash assistance, such as electronic cash, which is value sent to beneficiaries that can be converted into hard cash or spent without restrictions (e.g. mobile money, pre-paid cards, bank transfers); and electronic vouchers, which are sent to beneficiaries (through smart cards or mobile phones) that can be exchanged with approved merchants for approved items, with restrictions on spending possible.[138]

It is widely recognized that the effectiveness and appropriateness of humanitarian aid provided in cash depends on the situation (e.g. can individuals obtain the items they need in a particular situation?).[139] Although some concerns have been raised about Cash Transfer Programmes (e.g. inflation of the local market), there is evidence supporting these programmes as a "good value for money compared to in-kind alternatives."[140]

Research has shown that the greater use of humanitarian cash transfers where appropriate, without restrictions and delivered as electronic payments wherever possible, has benefits such as the following:[141]

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

136 See Diagram of Key Cash Transfer Terminology, Cash Transfers Glossary, at: http://www.cashlearning.org/downloads/glossary-annex-1.pdf.

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

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

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

140 *ibid*.

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

However, a number of difficulties and challenges also exist. Launching Cash Transfer Programmes in some Humanitarian Emergencies may not be an optimal solution (for example, in cases where basic goods are not available, where local authorities oppose this type of humanitarian aid, or where the relevant market is at a risk of inflation).[142] Often cash transfers may be part of bigger humanitarian assistance programme, including measures providing protection, sanitation or health services.[143] Finally, for Cash Transfer Programmes to function, Humanitarian Organizations need to process individuals' Personal Data. This poses inherent privacy-related threats and risks associated with the collection and handling of beneficiaries' Personal Data, in particular in light of the complex data flows they involve.

9.2 Application of basic data protection principles

The inherent privacy-related threats and risks associated with the collection and handling of beneficiaries' Personal Data for Cash Transfer Programmes can arise from inadequate organizational and technical data security measures. Personal Data collected for Cash Transfer Programmes can involve a variety of data sets that may not have been necessary for other types of humanitarian aid.[144] These data are shared with private entities to enable the distribution of financial aid. With an increasing number of Humanitarian Organizations opting for cash transfers programmes to provide assistance, there is a pressing need to consider the impact (e.g. will individuals receiving financial aid be subject to discrimination) and measures mitigating the risks associated with the Personal Data Processing needed to distribute this type of aid.[145]

Data protection issues result from the fact that data are collected, stored and cross-matched by Data Controllers or Data Processors during cash assistance programming operations. The Personal Data collected during the process typically include the following: name, surname, mobile phone number, "Know Your Customer"[146] data, geolocation/other phone metadata and Biometrics. Humanitarian Organizations may also collect data related to socioeconomic factors or vulnerabilities for the purposes of targeting assistance. This data, once collected and stored, may enable Processing for other purposes and/or other types of data Processing, such as Data Analytics or data mining.[147]

The complexity of the flow of data between Humanitarian Organizations and partner organizations involved in Cash Transfer Programmes also gives rise to data protection issues, which are dealt with in the section on data sharing below.[148]

9.3 Basic principles of data protection

The basic principles of data protection constitute the baseline to be respected while engaging in any type of Personal Data Processing. These include the principle of the fairness and lawfulness of the Processing, the principle of transparency, the purpose limitation principle, the data minimization principle and the data quality principle.[149]

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

142 *ibid*., page 11.
143 *ibid*., page 11.
144 Cash Learning Partnership, *Protecting Beneficiary Privacy, Principles and operational standards for the secure use of personal data in cash and e-transfer programmes*, page 4: http://reliefweb.int/sites/reliefweb.int/files/resources/calp-beneficiary-privacy-web.pdf.
145 *ibid*, page 4.
146 See Glossary and PWC, Know Your Customer: *Quick Reference Guide:* http://www.pwc.co.uk/fraud-academy/insights/anti-money-laundering-know-your-customer-quick-ref.html.
147 See Chapter 6: Data Analytics and Big Data.
148 See Section 9.5 Data sharing.
149 See also Chapter 2: Basic principles of data protection.

9.3.1 Legal bases for Personal Data Processing

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

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

Obtaining the valid informed Consent[150] of beneficiaries in Cash Transfer Programmes can be challenging, due to the amount and complexity of information that would need to be provided to ensure the beneficiaries fully appreciate the risks and benefits of Processing. In addition, as with other cases when Personal Data are collected as a prerequisite for assistance to be provided to beneficiaries, unless an alternative method of providing assistance is also made available, it can be argued that an individual in need of assistance has no real choice as to whether to give Consent or not and, accordingly, Consent may not be considered valid.

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

If Consent is not possible, then another legal basis could be used, as set out below, and beneficiaries should at least be informed individually or collectively as to the nature of the programme being provided, what information is being collected, by whom and why, and which Data Processors are involved.

Humanitarian Organizations should:[151]

- Aspire to obtain the active and informed Consent of beneficiaries for the use of their Personal Data in cash and e-transfer programmes.

150 See Section 3.2 Consent.

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

- Only use alternatives to active and informed Consent where obtaining it is impractical or valid Consent cannot be obtained for other reasons set out herein. Legitimate reasons for not seeking active and informed Consent include urgency, or if the circumstances of the distribution make "active and informed Consent" meaningless.
- If possible, ensure that valid Consent can be provided or offer an alternative method of assistance for the individuals who are not comfortable with the data flows and/or stakeholders involved in the Cash Transfer Programme.

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

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

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

9.3.2 Purpose limitation and Further Processing

At the time of data collection, the Humanitarian Organization concerned must determine and set out the specific purpose/s for which data are processed.[152] The specific purpose/s should be explicit and legitimate and, in the case of Cash Transfer Programmes, could include the provision of humanitarian assistance or, in case of cash for work grants, for example, the protection of water and habitat.

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

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

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

152 See Section 9.3.1 Legal bases for Personal Data Processing.

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

Additional purposes that may be involved in the Processing by or of interest to commercial processors (e.g. financial institutions and mobile phone operators) should also be considered. This may potentially include: cross-checking lists of beneficiaries against lists of designated persons, retention of metadata for law enforcement purposes, profiling beneficiaries for credit-worthiness, etc. The following consequences would ensue should commercial Data Processors be obliged or in a position to process Personal Data for purposes other than the exclusively humanitarian purpose envisaged:

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

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

EXAMPLE:
In the case of a cash transfer programming system deployed for aid distribution by a Humanitarian Organization, to which purpose the individuals concerned have consented, the same system cannot be used to transmit participants' data to donors of the Humanitarian Organization for cross-referencing purposes.

9.3.3 Data minimization

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

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

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

An example of best practice in cash assistance programmes is for the Humanitarian Organization to transfer, when feasible, a unique identifier (from which the receiving entity cannot identify the final beneficiary) and the amount of cash to be distributed to the commercial service provider (e.g. bank or mobile network operator), so as to limit the risks to the individuals concerned.

9.3.4 Data retention

Humanitarian Organizations are advised to ensure that beneficiary data are not held (whether by them or by Third Party Data Processors) for longer than is required to fulfill the specific purposes for which they were collected, un-

less retention is potentially useful for repeat distributions. The Personal Data of beneficiaries who have left the programme should be deleted both by the organization, its Data Processors, and any Third Parties that have had access to the data. The Humanitarian Organization should verify data deletion by the commercial service provider, as far as this is possible. Any information that is deemed necessary to keep at the end of a programme should only be kept if it is related to data for which there is a legitimate purpose, such as possible future programmes, auditing or reporting purposes, monitoring and evaluation. Ideally, and to the extent that this is meaningful, data retained for these reasons, should be aggregated and/or anonymized.

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

9.3.5 Data security

In order to avoid potential misuse of the Personal Data collected and processed during cash assistance programmes, it is essential that adequate and proportionate security measures are implemented. Humanitarian Organizations are advised to implement appropriate technical and operational security standards for each stage of the collection, use and transfer of beneficiary data, and processes should be put in place for the protection of beneficiary Personal Data from loss, theft, damage or destruction; this includes back-up systems and effective means to respond to security breaches and prevent unauthorized access, disclosure or loss.[153]

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

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

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

9.4 Rights of Data Subjects

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

153 See Section 2.8 Data security and Processing security.

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

9.5 Data sharing

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

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

- "Know Your Customer" (KYC) obligations requiring the collection of more Personal Data than is strictly necessary for the purposes of providing assistance.
- Obligations to cross-check KYC information against lists of designated persons established by local authorities, including entities potentially involved in a conflict or situation of violence. This process may potentially be monitored by public authorities, and may involve reporting obligations. This in turn gives rise to questions as to inclusion (i.e. can beneficiaries be excluded from an assistance programme on the basis of a match being found) and compromise the neutrality and independence of Humanitarian Action.
- Collection of additional data as part of the process, such as geolocation or unique telephone identifiers and other mobile network metadata, when mobile phone operators are involved.
- Retention obligations incompatible with the information provided by Humanitarian Organizations at the time of collection.
- Additional commercial purposes, such as profiling individuals for credit worthiness or advertising.
- Additional obligations imposed on them by national law.

Privileges and immunities are also of great significance with respect to Cash Transfer Programmes. In this regard, the provisions of Section 10.9 Privileges and immunities and the cloud should be considered for Cash Transfer Programmes.

9.6 International Data Sharing

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it in cash assistance programmes, as discussed in Chapter 4: International Data Sharing. Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out.

9.7 Data Controller/Data Processor relationship

The deployment of a Cash Transfer Programme by a Humanitarian Organization may involve local or international commercial service providers for project implementation. Humanitarian Organizations may also cooperate among themselves in sharing databases of the information collected via these operations. It is thus crucial to determine which parties actually determine the purposes and means of data Processing (and thus are Data Controllers), and which merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers. When the roles have been clearly defined and the corresponding tasks assigned, data sharing across Humanitarian Organizations and/or national borders and/or third (private or state) bodies should generally be covered by appropriate contractual arrangements.

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

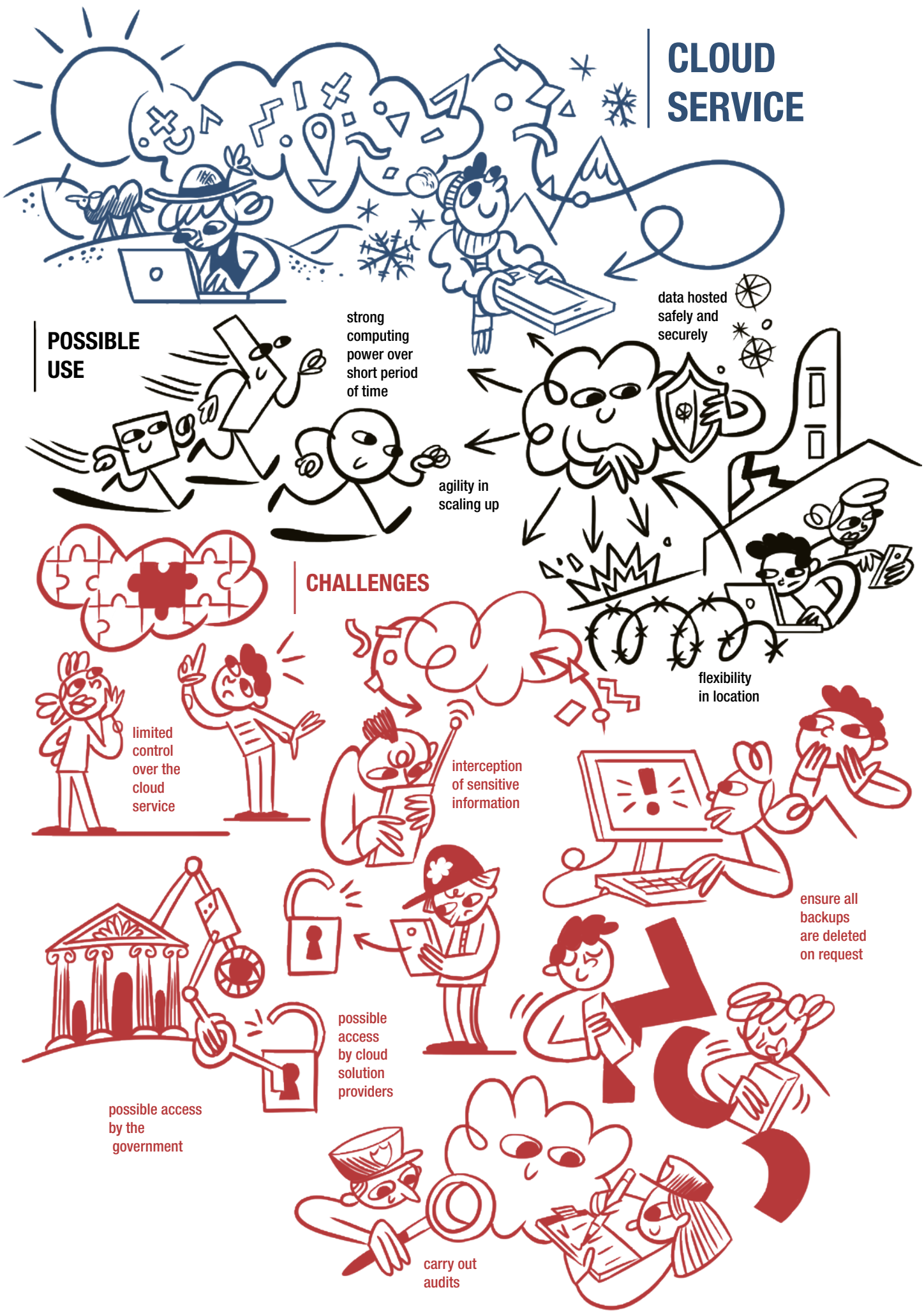
9.8 Data Protection Impact Assessments

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

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

A template DPIA for cash transfer programming has been developed by the Cash Learning Partnership.[154]

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


CLOUD SERVICE
POSSIBLE USE
strong computing power over short period of time
agility in scaling up
data hosted safely and securely
flexibility in location
CHALLENGES
limited control over the cloud service
interception of sensitive information
ensure all backups are deleted on request
possible access by cloud solution providers
possible access by the government
carry out audits

Chapter 10:
CLOUD SERVICES

10.1 Introduction

The most widely used definition of "cloud computing" is the one published by the US National Institute of Standards and Technology (NIST),[155] according to which, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The NIST document defines three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four deployment models: public, private, community and hybrid cloud environments,[156] although it should be borne in mind that new models are being developed all the time.

Cloud computing can facilitate and accelerate the creation and Processing of large collections of data and the production of new services and applications; it also makes deployment more agile. As humanitarian assistance is driven by information, this new, alternative data Processing paradigm has become a helpful tool for Humanitarian Organizations. Its benefits include access to large amounts of computing power over short periods of time, elasticity and flexibility about the location and flow of data, and cost savings.[157]

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

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

The data protection implications of cloud computing were highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Cloud Computing, adopted in Uruguay in 2012.[158]

In addition, those Humanitarian Organizations that enjoy privileges and immunities under international law should be aware that outsourcing Personal Data Processing to a Third Party cloud service provider may put their data at risk of loss of such privileges and immunities. More details on the possible implications of privileges and immunities in a cloud environment are set out in Section 10.9 Privileges and immunities and the cloud below.

The three main types of cloud service models can be described as follows:[159]

- Infrastructure as a Service (IaaS): an IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.

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

156 European Data Protection Supervisor (EDPS), Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", page 4: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

157 Dara Schniederjans and Korey Ozpolat, *An Empirical Examination of Cloud Computing in Humanitarian Logistics,* Working Paper: http://www.cba.uri.edu/research/brownbag/spring2013/documents/DaraS2013329paper.pdf.

158 See: https://icdppc.org/document-archive/adopted-resolutions/.

159 Information Commissioner's Office, *Guidance on the use of Cloud Computing*, 2012, pages 5-6: https://ico.org.uk/for-the-public/online/cloud-computing/.

- Platform as a Service (PaaS): a PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run on that platform or another instance of it. The platform may in turn be hosted on a cloud IaaS.
- Software as a Service (SaaS): a SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

There are also different types of cloud infrastructure. A private cloud is operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally. In a public cloud, the services are rendered over a network that is open for public use. A hybrid cloud is a composition of two or more clouds that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

Each of these models has advantages and disadvantages. A public cloud is more accessible, as the information is stored offsite and therefore is available from anywhere via the internet. It offers the ability to scale up server capacity at short notice and can potentially save money. It can also be reviewed regularly with security and performance updates and improvements. On the other hand, as a public cloud is dependent on internet connectivity there is the risk of losing control over data because of unknown or unauthorized data transfer from one jurisdiction to another, false deletion of data, retention after the termination of services, hacking and security attacks. It is difficult to identify where the data are stored in a public cloud at a particular point in time, and deletion is almost never possible because of the many unmonitored back-ups. In addition, there are many privacy and confidentiality concerns, such as the fact that the Processing may be subject to a range of different applicable legislation which could mandate compulsory and unauthorized release of data and the potential for authorities to exercise jurisdiction.

In a private/internal cloud, data are kept within the organization's internal network, and therefore are not publicly accessible. It offers a more controlled environment and a limited number of users, so creating less risk of third-party disclosure. A private cloud can have the same usability, scalability and flexibility as a public cloud. Its disadvantages, though, are the cost and the fact that it may not have the latest performance and security upgrades/improvements.

A hybrid cloud allows organizations to determine which option to use, depending on the classification of information to be stored. Less sensitive information is usually sent to a public cloud, whereas more sensitive and confidential information is kept on a private or internal cloud. While this model offers cost savings, scalability, security and performance updates/improvements, it entails the same risks as a public cloud in terms of loss of control over data and unauthorized disclosure.

10.2 Responsibility and accountability in the cloud

The cloud client – provider relationship is a Data Controller – Data Processor relationship.[160] However, in exceptional cases the cloud provider may act as a Data Controller as well, in which case it has full (joint) responsibility for the data Processing and must comply with all relevant legal obligations for data protection. As the Data Controller, the cloud client (i.e. the Humanitarian Organization) is responsible for complying with legal obligations stemming from data protection law. Furthermore, the cloud client is responsible for selecting a cloud provider that complies with data protection legislation.

160 See Section 10.7 Data Controller/Data Processor relationship.

The notion of accountability expresses the direct compliance obligations that Data Controllers and Data Processors have under data protection law. This means that they must be able to ensure and demonstrate that their Processing activities comply with the relevant legal requirements, through the adoption and implementation of appropriate data protection policies and notices.

EXAMPLE:
When a Humanitarian Organization contracts with a cloud provider to store Personal Data in the cloud, it will remain liable to the Data Subjects for any breaches of data protection that the provider commits. It is therefore essential for the Humanitarian Organization to take the following steps before Personal Data are stored in a cloud:

- undertake a DPIA on the proposed storage of Personal Data in the cloud, and be prepared to cancel the project if the results show that this would cause undue risk for individuals' data protection;
- perform due diligence on the cloud service provider to ensure that the provider will use due care and takes data protection seriously;
- discuss data protection openly with the provider and assess whether the provider seems ready and able to fulfil their data protection obligations;
- carefully review the contract with the provider before signature and ensure that it contains adequate data protection language; and
- for Humanitarian Organizations enjoying privileges and immunities, ensure that such privileges and immunities are properly built into the cloud solution design, and are respected.

10.3 Application of basic data protection principles

All data protection principles apply to cloud services; special attention is paid here to a number of issues that are of particular relevance.

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

10.3.1 Legal bases for Personal Data Processing

Before engaging a cloud provider Humanitarian Organizations need to demonstrate that one of the following legal bases is present:[161]

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

It is important in this regard to differentiate between the initial Processing of the Personal Data by the Humanitarian Organization and its Processing in the cloud. The Humanitarian Organization must have a legal basis for collecting and Processing the Personal Data in the first place, which can be any of the legal bases referred to in Chapter 3: Legal bases for Personal Data Processing. In addition, there must be a separate legal basis for the Processing in the cloud. There should be a case by case assessment of each legal basis in each specific situation or humanitarian operation and whether it can be extended to the cloud, either as an "extra" legal basis or cumulatively.

161 See Chapter 3: Legal bases for Personal Data Processing.

Even when the vital interest of the Individuals is a sufficient legal basis for collecting Personal Data, there must also be a legal basis for placing the data in the cloud.

EXAMPLE:
A Humanitarian Organization collects Personal Data from vulnerable individuals on the basis that it is in their vital interest. In order to provide humanitarian services more efficiently, it then wants to store the data in a private cloud, and to this end engages a cloud service provider. The vital interest of the individuals is a sufficient legal basis for collecting the Personal Data, but there must be a legal basis for placing the data in the cloud as well. Vital interest might not be a sufficient legal basis for placing the data in the cloud, since the humanitarian services could be performed without this; rather, the purpose of putting it in the cloud is to make the provision of humanitarian services more efficient. A possible legal basis for using the cloud provider could be that it is in the legitimate interest of the Humanitarian Organization and this interest is not outweighed by the fundamental rights of the Data Subjects whose data are being processed. This argument is strengthened by the fact that a private cloud is being used. A DPIA should be performed to confirm the legal basis.

10.3.2 Fair and lawful Processing

Personal Data must be processed lawfully and fairly. The lawfulness of the Processing refers to the identification of an appropriate legal basis,[162] while the requirement for fairness is a broad principle that is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations using cloud services should bear in mind that these Principles apply during all stages of Processing (i.e. collection, Processing and storage).

10.3.3 Purpose limitation and Further Processing

Humanitarian Organizations must determine and set out the specific purposes of Personal Data Processing. The purposes of the Processing need to be clarified and communicated to individuals at the time of collection.

Humanitarian purposes offer a wide basis upon which to justify Further Processing operations. Compatibility would, however, not be found if the risks for the individuals concerned outweigh the benefits of Further Processing. This depends on the particular case. For example, circumstances leading to a finding of incompatibility include risks that the Processing may run counter to the significant interests of the person to whom the information relates or of his/her family, in particular when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or their reputation.

162 See Section 10.3.1 Legal bases for Personal Data Processing.

In cloud computing environments, the cloud client is responsible for determining the purpose(s) of the Processing prior to the collection of Personal Data from the Data Subject and must inform the Data Subject accordingly. Based on the prohibition that the cloud client must not process Personal Data for other purposes that are inconsistent with the original ones, a cloud service provider cannot unilaterally decide or arrange for Personal Data (and its Processing) to be transmitted automatically to unknown cloud data centres. Furthermore, the cloud service provider cannot use Personal Data for its own purposes (such as, for example, marketing, carrying out research for other purposes or profiling).

Moreover, Further Processing that is incompatible with the original purpose(s) is also prohibited for the cloud provider and its sub-contractors. A typical cloud scenario may easily involve a larger number of sub-contractors. In order to mitigate the risk of Further Processing, the contract between cloud provider and cloud client should include technical and organizational measures and provide assurances for the logging and auditing of relevant Processing operations on Personal Data that are performed by employees of the cloud provider or the sub-contractors.

10.3.4 Transparency

Transparency is an aspect of the fair and legitimate Processing of Personal Data and is also closely related to the provision of information to Data Subjects. The cloud client is obliged to provide Data Subjects, whose Personal Data or data related to them are collected, with detailed information; this includes the cloud client's identity, address and the purposes of the Processing; the recipients or categories of recipients of the data, including Data Processors, insofar as such further information is necessary to guarantee fair Processing; and information about their rights.

Transparency must also be guaranteed in the relationship(s) between cloud client, cloud provider and sub-contractors (if any). The cloud client can assess the lawfulness of the Personal Data Processing in the cloud only if the provider informs the client about all relevant issues. A Data Controller contemplating the engagement of a cloud provider should carefully check the provider's terms and conditions and assess them from a data protection point of view.

Another aspect of transparency in cloud computing is the fact that the cloud client must be informed about all the sub-contractors involved in the provision of the respective cloud service, not merely those with which it is in a direct contractual relationship, and the locations of all data centres in which Personal Data may be processed.

10.3.5 Data retention

Humanitarian Organizations are advised to ensure that Personal Data are not held (whether by them or by Third Party Data Processors) for longer than is required unless they have clear, justifiable and documented reasons for doing so; otherwise, data held by the organization and any relevant Third Parties should be destroyed. Deletion or destruction after completion of their Processing or a carefully structured data retention policy is recommended. When the purposes for which the Personal Data were collected have been achieved, then the Personal Data should be deleted both by the organization and any Third Parties that have had access to the data, unless the Third Party has Consent to hold that data.

Data should only be retained in cloud services if they are related to a legitimate Processing purpose. Legitimate purposes in this regard might include possible future programmes, monitoring and evaluation, whereas for research purposes anonymized or aggregated data might be appropriate. Only the minimum

amount of data necessary should be retained, in accordance with the data minimization principle.

The responsibility to ensure that Personal Data are erased as soon as they are no longer necessary lies with the cloud client. Erasure of data is a crucial issue not only throughout the duration of a cloud computing contract, but also upon its termination. It is also relevant if a sub-contractor is replaced or withdraws. In such a case, the cloud client might either request a certificate of destruction by the cloud service provider or a certificate confirming that the data were transferred to a new cloud service provider.

The principle of data erasure is applicable to Personal Data irrespective of whether they are stored on hard drives or other storage media (e.g. backup tapes). Since Personal Data may be kept at the same time on different servers at different locations, it must be ensured that each instance is erased irretrievably (i.e. previous versions, temporary files and even file fragments should also be deleted).

Secure erasure of Personal Data requires that either the storage media are destroyed or demagnetized, or that the stored Personal Data are deleted effectively. Special software tools that overwrite Personal Data multiple times, in accordance with a recognized specification, should be used. The cloud client should make sure that the cloud provider ensures secure erasure in the above-mentioned sense and that the contract between the provider and the client contains clear provision for Personal Data erasure. The same holds true for contracts between cloud providers and sub-contractors.

10.4 Data security

Data security measures can be legal, technical and organizational. Legal measures may include not only contractual arrangements, but also Data Protection Impact Assessments (DPIAs). A holistic perspective must be adopted, which takes the following phases of contracting for cloud services into account:

- assessing the decision to use cloud computing (via DPIAs and a "go/no go" decision by management);
- the cloud service procurement process, including due diligence on prospective cloud service providers that takes both legal and technical perspectives into account;
- contracting (i.e. getting the right terms and conditions); and
- operating, maintaining and decommissioning the service.

A comprehensive data protection strategy is recommended and attention should be paid to data protection issues in all phases before, during and after contractual arrangements. This should include an overall assessment of the contractual framework, including service level agreements (SLAs), general (non-data protection) clauses (e.g. applicable law, variations to the contract, jurisdiction, liability, indemnification, etc.), and the general principle of "parallelism in/outside the cloud" (e.g. having the same data retention period for cloud or non-cloud Processing).

When a Humanitarian Organization decides to contract for cloud computing services, it should choose a cloud provider that can give sufficient guarantees for technical security and organizational measures governing the envisaged Processing, and ensure compliance with those measures. Furthermore, a written contract with the cloud service provider must be signed, as there must be a binding legal act to govern the relationship between the Data Controller and the Data Processor. The contract must at a minimum establish that the Data Processor is to follow the instructions of the Data Controller and that the Data Processor must implement technical and organizational measures to adequately protect Personal Data, in accordance with the applicable data protection law.

In order to ensure legal certainty, the contract between the Humanitarian Organization and the Data Processor should also contain the following core data protection clauses:

- Provision of information on the location of the data centres, the identity and location of sub-contractors, and on any subsequent changes to the nature of the Processing. This should include the subject and time frame of the cloud service to be provided by the cloud provider; the extent, manner and purpose of the Processing of Personal Data by the cloud provider; and the types of Personal Data processed.
- Details about the cloud client's instructions to be given to the provider, with particular regard to the applicable SLAs and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data. Note that a security incident does not necessarily constitute a data breach.
- There is an obligation to process Personal Data only for the explicitly mentioned and specified purposes, and to delete data at the end of the contract. There must be specification of the conditions for returning the data or destroying them once the service is concluded. Furthermore, it must be ensured that Personal Data are erased securely at the request of the cloud client.
- Confirmation, in case of a private cloud located outside the cloud client premises, that the data of the Humanitarian Organization are kept in separate servers.
- Specification of security measures that the cloud provider must comply with, depending on the risks represented by the Processing and the nature of the data to be protected.
- Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to the data.
- Obligation on the provider's part to support the client in facilitating the exercise of Data Subjects' rights to access, correct or delete their data.
- Obligation on the provider's part to respect the cloud client's privileges and immunities, if applicable.
- The contract should specify that Sub-Processors may only be commissioned on the basis of Consent that can be generally given by the Data Controller (cloud client), in line with a clear duty for the Data Processor to inform the Data Controller of any intended changes in this regard, with the Data Controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation for the cloud provider to name all the sub-contractors commissioned. It must be established that contracts between the cloud provider and sub-contractors reflect the stipulations of the contract between cloud client and cloud provider (i.e. that Sub-Processors are subject to the same contractual duties as the cloud provider). In particular, it must be guaranteed that both the cloud provider and all sub-contractors act only on instructions from the cloud client. The chain of liability should be clearly set out in the contract.
- Audits should be conducted during and at the end of the contract by the cloud client. The contract should provide for logging and auditing of relevant Processing operations on Personal Data that are performed by the cloud provider or the sub-contractors.
- A general obligation on the provider's part to give assurance that its internal organization and data Processing arrangements (and those of its Sub-Processors, if any) are compliant with the applicable national and international legal requirements and standards.

With regard to the technical aspects of data security, the following are some important considerations for Humanitarian Organizations to bear in mind:[163]

- **Availability:** Providing availability means ensuring timely and reliable access to Personal Data. Availability in the cloud can be threatened by accidental loss of network connectivity between the client and the provider or of server performance caused by malicious actions such as (Distributed) Denial of Service (DoS) attacks. Other availability risks include accidental hardware failures both on the network and in the cloud Processing and data storage systems, power failures or other infrastructure problems. Data Controllers should therefore check that the cloud provider has adopted reasonable measures to cope with the risk of interferences such as backup internet network links, redundant storage and effective data backup mechanisms.
- **Integrity:** Integrity relates to the maintenance of data quality which should not be maliciously or accidentally altered during Processing, storage or transmission. For IT systems, integrity requires that Personal Data undergoing Processing on these systems remain unmodified. Personal Data modifications can be detected by cryptographic authentication mechanisms such as message authentication codes, signatures or cryptographic hash functions. Interference with the integrity of IT systems in the cloud can be prevented or detected by means of Intrusion Detection and Prevention Systems (IDS/IPS). These security tools are particularly important for the open network environments in which clouds usually operate.
- **Confidentiality:** In a cloud environment, encryption can significantly contribute to the confidentiality of Personal Data if applied correctly, although it does not render Personal Data irreversibly anonymous. It is simply a tool for the cloud client to ensure that the Personal Data they are responsible for can only be accessed by authorized persons who have the correct key. Personal Data encryption should be used for all data "in transit" and, when available, to data "at rest". This applies particularly for Data Controllers who plan to transfer Sensitive Data. Communications between cloud provider and client, as well as between data centres, should also be encrypted. When encryption is chosen as a technical measure to secure data, it is also important to guarantee the security of the key. Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication). Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and sub-contractors.
- **Isolation (purpose limitation):** Isolation is an expression of the purpose limitation principle. In cloud infrastructures, resources such as storage, memory and networks are shared among many users. This creates new risks for data disclosure and illegitimate Further Processing. Isolation is meant to address this issue and ensure that data are not used beyond their initial original purpose and to maintain confidentiality and integrity. Isolation is achieved by adequate governance of the rights and roles for accessing Personal Data, and should be reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g. no user or administrator should be authorized to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for legitimate purposes (least privilege principle).
- **Intervenability:** Data Subjects have the rights of access, rectification, erasure, blocking and objection, as discussed below.[164]

163 Adapted from Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, WP 196, 1 July 2012, pages.14-17: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

164 See Section 10.5 Rights of Data Subjects.

- **Portability:** The use of standard data formats and service interfaces by the cloud providers is very important, as it facilitates interoperability and portability between different cloud providers. Therefore, if a cloud client decides to move to another cloud provider, any lack of interoperability may make it difficult or impossible to transfer the client's (personal) data to the new cloud provider, which is known as "vendor lock-in". The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a cloud service. Data portability also refers to the ability of a Data Subject to obtain from the Data Controller a copy of data undergoing Processing in a commonly-used, structured, electronic format. In order to implement this right, it is important that, once the data have been transferred, no trace is left in the original system. In technical terms, it should become possible to verify the secure erasure of data.

The following are further IT security principles for Humanitarian Organizations to consider when moving to the cloud.[165]

10.4.1 Data in transit protection

Data transmissions must be properly secured against eavesdropping and tampering. This is relevant not only for connections between the premises of the organization and the cloud application, but also for data paths inside the service and for connections between the application and other services (API).[166] A common solution is the encryption of network traffic, using network level traffic encryption (VPN),[167] transport layer security (TLS) or application level encryption. Due care must be taken to choose the correct protocols and implementation of encryption, as well as in the management of secret keys for the encryption itself. Dedicated fibre optic connections can also be used, where they are convenient and the situation allows it.

10.4.2 Asset Protection

Protecting assets in cloud situations is different from protecting them in on-site arrangements. Consequently, several specific points need to be considered when evaluating a cloud solution.

10.4.2.1 Physical location

It is important to know the physical location(s) of data storage in order to understand which legislation applies, but also the likelihood of specific threats, such as power and network outages, actions by hostile groups and organizations, and other country-specific threats. It is therefore important to obtain a detailed statement regarding the physical location of data centres and be aware that data exchanges between data centres in different locations can happen without the organization's knowledge.

For Humanitarian Organizations with privileges and immunities, it is also essential that the country in which data centres are stored has a legal obligation to respect privileges and immunities, and is known to respect them in practice.

10.4.2.2 Data centre security

In cloud service arrangements, the physical security of data centres is fully controlled by the service provider; it is therefore important to have a clear idea of the security at the premises in which the data and applications are stored. This

165 The authors express their gratitude to ICT Legal Consulting for permission to use the material on cloud security. Adapted from UK National Cyber Security Centre, Guidance *Implementing the Cloud Security Principles*, 2016: https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience.

166 API – an application programming interface is a set of subroutine definitions, protocols and tools for building application software: https://en.wikipedia.org/wiki/Application_programming_interface.

167 VPN – A virtual private network extends a private network across a public network, such as the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network: https://en.wikipedia.org/wiki/Virtual_private_network.

can be achieved by verifying the certifications (if any) obtained by the data centre and/or the contractual obligations underlying the relationship between the cloud service provider and the organization. The level of security guaranteed should match the level of security required by the application to be hosted in the cloud. Physical inspection could give useful information, but is unlikely to be possible in most cloud environments.

10.4.2.3 Data at rest security

The level of security for data at rest depends on the type of service required and other arrangements with the service provider. However, it is reasonable to assume that data will be stored in shared storage media, so a clear statement of the service provider about the protection level and how it is achieved is required, along with any related Third Party certification. However, it is recommended not to rely only on cloud provider security for data at rest, at least for most Sensitive Data, but to add additional layers of protection, such as encryption.

10.4.2.4 Data sanitization

Cloud environments are characterized by a high frequency of provisioning, deletion and migration of resources; in other words, data and applications can easily be moved around different parts of the shared infrastructure. If not correctly managed, this could lead to data disclosure, as other customers' applications will likely be run on the same hardware previously used by Humanitarian Organizations. Moreover, data could remain indefinitely in the cloud infrastructure. Measures should be taken to control this threat: using dedicated resources and/or verifying with the provider which measures are in place to erase or otherwise sanitize the data. The use of encryption, independently from the service provider, could offer an additional layer of protection.

10.4.2.5 Equipment disposal

Equipment disposal is closely related to the previous point and a fair level of confidence should be achieved that no data or information could remain stored or possibly be disclosed when hardware is decommissioned or disposed of. The cloud provider should give some guarantee that this requirement can be met or other measures must be adopted (i.e. encryption).

10.4.2.6 Availability

Cloud services must offer the required level of availability; service level agreements (SLAs) are of paramount importance in this respect. The agreement should also be examined in terms of liabilities and responsibility. Verification of any publicly available information, which could help in ascertaining the actual reliability of the service offered, is recommended.

10.4.3 Separation between users

In a cloud environment, the service provider is responsible for guaranteeing user separation. However, it is important when evaluating a cloud provider, and even more so when the provider and the related technology are not widely known, to assess the technology used and gather any information that can help in understanding how the separation is ensured. The separation is affected by several factors, such as the service model, the deployment model (public versus private cloud) and other factors. To assess the effectiveness of separation measures, a penetration test can be useful, but only to a limited extent: it is valid only for the specific time when the test is carried out and it only gives an indication about known issues. A background check of previous incidents and their management by the provider can also be extremely useful.

10.4.4 Governance

The service provider should have a proper security governance framework, as this is the basis to control and coordinate all security efforts, and to manage

changes in threat and developments in technology. The provider should then demonstrate that it possesses the required elements that are typically associated with a C* level manager (e.g. CSO, CISO, CTO) in charge of cloud security; that it has a properly implemented framework for security governance; that security and security risks are included in general risk and financial management; and that it complies with regulations and legal requirements. Conformance with recognized standards should be assessed.

10.4.5 Operational security

The cloud provision service must be operated in accordance with strict security requirements and security must be embedded in standard operating procedures. The main elements are:

- configuration and change management, to control what is in the production environment and related changes, to perform the required tests and receive proper authorization before making changes;
- vulnerability management, to assess, identify and correct security issues that can arise in services and infrastructure;
- monitoring, to detect anomalies, attacks and unauthorized actions that can undermine the security of the services; and
- incident management: when an incident occurs, the service provider must be able to address it by taking adequate measures in order to mitigate, contain and properly correct the issue. This includes communications and reports to the customers and law enforcement authorities.

10.4.6 Personnel

The cloud service provider must have in place measures to assess the trustworthiness of the personnel involved in the service management. Proper background checks and screening should be implemented for any privileged or sensitive role. Operators should be trained and must understand and acknowledge their responsibilities.

10.4.7 Development

Service providers usually develop large parts of their infrastructure. They should employ best practices and industry standards to ensure that threats are evaluated during development; guidelines for secure design, coding, testing and deployment should be in place.

10.4.8 Supply chain

Cloud providers often use Third Party products and services to integrate or manage the services they offer. Any weakness along the supply chain can compromise the security of the entire cloud service and applications. The provider should describe how the third-party suppliers are screened; the acceptance process for services and products; how security risks are managed; how the security posture of the service providers is verified; and how spare parts, updates and other changes are verified. This process is made even more important by the fact that cloud services can be layered, relying on other service providers lower down the chain. If possible, verification of the suppliers should be performed or agreements should be in place to prevent the cloud provider from using Third Party suppliers not acceptable to the organization.

10.4.9 User management

Depending on the service offered, the authorization process may, in part, be managed by the cloud provider. This process should be assessed to verify its compliance with best practices, regulations and the organization's needs, in order to ensure secure access to management interfaces. These interfaces allow the performance of actions that can be considered equivalent, to a certain extent,

to physical actions performed inside a traditional data centre; consequently, such actions need to be carefully guarded. Privileges should be fine-grained, so as to ensure the correct management of roles and privileges.

10.4.10 Identity and authentication

As with user management, access to any service interface should be strictly guarded. Implementation of identification and authorization processes should be assessed to conform to the security needs of the organization. Examples of different approaches are: two factor authentication, use of TLS client certificates, single sign-on systems, etc. The methods adopted must be kept up to date with developments in security and the growing sophistication of the threats.

10.4.11 External interfaces

When management interfaces are exposed, this increases the attack surface available to hostile entities. The security of those interfaces should therefore be assessed against this threat; the availability of solutions such as private networks or equivalent measures to access private interfaces should be assessed.

10.4.12 Service administration

The architecture and management of administration systems should be carefully designed and implemented, as these systems are highly valuable for attackers. Thus, a description of administration systems management and procedures can be useful to assess the security posture of the service provider.

10.4.13 Audits

The service provider should make available the results of independent audits or allow the organization to ask for an independent assessment or audit. Audit data regarding the services (performance, downtime, security incidents and so on) should also be available for scrutiny.

10.4.14 Service usage

The organization must have a clear understanding of the interactions with the cloud service: interfaces, data exchanges, authorization process for users, administration, workloads and any other aspect that can influence the service considered as the sum of cloud and organization activities. A detailed assessment of data flow, processes and architectures must be conducted prior to implementing a cloud solution. Proper procedures must be designed and implemented, personnel must be trained, and operators should be provided with the requisite knowledge about the cloud solution, the usage, the relationship with the organization and other information related to correct use and management of the cloud solution.

10.5 Rights of Data Subjects

Data Subjects also have the rights of access, rectification, erasure and objection with regard to their Personal Data processed in the cloud.[168] The Humanitarian Organization must verify that the cloud provider does not impose technical and organizational obstacles to these requirements, even in cases when data are further processed by sub-contractors. The contract between the client and the provider should require that the cloud provider facilitates the exercise of the Data Subjects' rights and ensures that the same exercise of these rights is safeguarded in its relationship with any sub-contractor.

10.6 International Data Sharing

By their very nature cloud services involve International Data Sharing of Personal Data with various parties located in different countries. Data protection law restricts International Data Sharing; Humanitarian Organizations should

168 See Section 2.11 Rights of Data Subjects.

therefore ensure that the use of cloud services is in compliance with any laws to which they are subject, if any, and with their own internal policies. This means, for example, that any contract with a cloud provider should indicate how the provider complies with legal requirements concerning International Data Sharing (e.g. through the use of contractual clauses with its entities and with sub-contractors). Performing a DPIA[169] prior to International Data Sharing could further strengthen the lawfulness of such Processing from a data protection perspective.

10.7 Data Controller/Data Processor relationship

As discussed in Section 4.5 above,[170] the relationship between a Humanitarian Organization that puts Personal Data in the cloud and a cloud provider that it contracts with to do so is, generally speaking, that of a Data Controller and a Data Processor. However, in practice these roles may be more difficult to categorize than is at first apparent, as this will depend on how much discretion the cloud provider has, and which should be defined in the agreement between the provider and the client. What is crucial is that these uncertainties should not affect the rights of Data Subjects, meaning that Humanitarian Organizations should be as transparent as possible about their use of cloud services and not allow cloud providers to disadvantage Data Subjects.

The use of cloud services by a Humanitarian Organization routinely involves the cloud provider hiring Sub-Processors. The contract with the provider should specify that Sub-Processors may only be used on the basis of Consent given by the Data Controller (i.e. the Humanitarian Organization). The Data Processor (cloud provider) should have a clear duty to inform the Data Controller of any changes in this regard, with the Data Controller retaining the option of objecting to such changes or terminating the contract.

10.8 Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of data protection regulations and applicable risks are addressed. It is essential to carry out specific DPIAs tailored to cloud computing whenever there is interest in using cloud services.[171] DPIAs should clarify the Processing details and specifications, and also focus on the risks posed by it as well as on mitigating measures. In this respect, it is important to note that DPIAs should be undertaken prior to the use of cloud services.

10.9 Privileges and immunities and the cloud

Beyond the considerations above, Humanitarian Organizations benefitting from privileges and immunities should also consider that data placed in the cloud may jeopardize the protection of such privileges and immunities, unless specific legal, technical and organizational measures are put in place. This consideration is key, particularly given that in Humanitarian Emergencies, the privileges and immunities of a Humanitarian Organization may be the first line of protection for the Personal Data of vulnerable individuals, particularly in conflicts and other situations of violence.

Humanitarian Organizations should consider implementing the legal, organizational and technical measures suggested below, to ensure that their privileges and immunities are adequately protected in a cloud environment.

169 See Section 10.8 Data Protection Impact Assessments.
170 See Section 4.5 Data Controller/Data Processor relationship.
171 See Chapter 5: Data Protection Impact Assessments (DPIAs).

10.9.1 Legal measures

- Data should be hosted and processed by external Data Processors exclusively in jurisdictions where the privileges and immunities of the organization are formally recognized by status agreements recognising the inviolability of files, archives, correspondence and communication wherever and by whomever the organizations' data are held, as well as immunity from every form of legal process. This legal protection should ideally be backed by a track record of such privileges and immunities being consistently respected.
- Data Processors and Sub-Processors should be bound by contractual obligation to notify any requesting authorities who seek to access data, that the data in question is covered by a Humanitarian Organization's privileges and immunities; to decline any requests for access by authorities, whether informal, administrative or through judicial process, and to re-direct the authorities' request to the Humanitarian Organization; to immediately notify the Humanitarian Organization of any request for access to its data, whether informal, administrative or through judicial process, the identity of the requesting authority and status of the request; and to assist the Humanitarian Organization with the provision of any information and documentation that may be necessary as part of any proceedings, whether informal, administrative or through judicial process, that may be required by the Humanitarian Organization in order to assert its privileges and immunities over the relevant data.

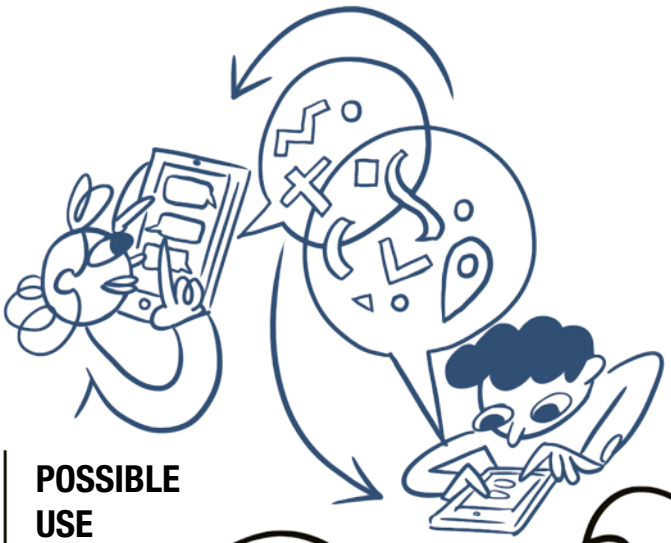
10.9.2 Organizational measures

- The data of the Humanitarian Organization should be held in segregated servers, and the data should be segregated from the data of other clients of the Data Processors and Sub-Processors.
- The servers hosting the data of the Humanitarian Organizations should be clearly marked with the emblem of the organization and the indication "Legally Privileged Information" should be marked on the servers.
- Where possible, the servers hosting the data of Humanitarian Organizations should only be accessed with the authorization of both the Data Processors and of the Humanitarian Organization.
- Staff of the Data Processor and Sub-Processors should be properly informed of the privileged status of the data, and trained on the procedure to follow in case of requests for access by Third Parties.

10.9.3 Technical measures

- Data hosted in a cloud environment should be encrypted and encryption keys held only by the Humanitarian Organization.
- If the cloud solution envisaged is a SaaS, and the Data Processors and Sub-Processors need to manage the service offered, arrangements should be made to ensure that such Data Processors and Sub-Processors may access the system to manage it, run updates, fix bugs and support users, without ever having access to clear (unencrypted) data.

MOBILE MESSAGING APPS



POSSIBLE USE

CHALLENGES

need for clear guidance on processing by humanitarian organizations of information gathered from messaging apps

lack of awareness about types of data processed

metadata could be accessed and analysed by third parties and used by them in ways detrimental to vulnerable individuals

Chapter 11:
MOBILE MESSAGING APPS

11.1 Introduction[172]

In their daily work, Humanitarian Organizations rely on multiple communication channels, including formal (e.g. radio and television), informal, unofficial and direct means of exchanging information. To employ the most appropriate communication channels in a given situation, Humanitarian Organizations have to understand the cultural background and needs of a particular society affected by a crisis and their means of communication.

In this respect, where such apps are widely used, their deployment by Humanitarian Organizations is particularly attractive, because it allows immediate communication with people affected by crisis or conflict, and helps to coordinate internal tasks and actions efficiently. This type of technology can enhance the effectiveness and efficiency of Humanitarian Actions and reach populations in remote or inaccessible locations. However, messaging apps are often employed without due consideration of the risks relating to Personal Data protection.

Migrants charge their mobile phones at a temporary Wi-Fi hotspot in a makeshift camp near the San Giovanni railway station in Como, Italy, August 2016.

Despite the great functionality offered by mobile messaging apps, their use may entail significant data protection risks. It seems that in practice, Humanitarian Organizations sometimes deploy them ad hoc, without following any formal procedures underpinned by risk analysis or considerations of long term sustainability and management. Rather, the focus is on the Humanitarian Organizations' pressing information and communications needs. Insofar as this approach fails to include risk analysis, it runs counter to the guiding principles of Humanitarian Organizations, such as accountability, appropriateness, "do no harm", and due diligence. As is the case with any other communication channel, the adoption of mobile messaging apps requires the careful consideration of their benefits and risks. Questions to be included in such an analysis depend on the specific circumstances of a particular situation. For example, security concerns about Personal Data of individuals in a situation of political violence may differ greatly from security concerns in a natural disaster.

172 This chapter is based on the report *Humanitarian Futures for Messaging Apps*, ICRC, The Engine Room and Block Party, January 2017: https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

Mobile messaging apps installed on cellular phones or other smart devices may pose risks to individuals' right to Personal Data protection. This is because apps provide not only the possibility to exchange data between users, but also to process, aggregate, and generate huge amounts of data (e.g. metadata, location data and contacts). Some data protection regulators consider that risks to Personal Data Protection result from a combination of the following factors: 1) users' lack of awareness about the types of data they actually process on a smart device; 2) absence of user Consent; 3) poor security measures; and 4) the possibility of Further Processing.[173]

In line with the "digital proximity" imperative, i.e. Humanitarian Organizations seeking to be digitally where the beneficiaries are (just as they try to be physically), Humanitarian Organizations tend to deploy mobile messaging apps that are popular in a particular society at the time of a Humanitarian Emergency, such as WhatsApp, Facebook Messenger, Snapchat, Viber, Telegram and LINE. These proprietary cross-platforms are established service providers which may not be willing to customize their applications to meet the needs of Humanitarian Organizations. At the same time, deploying a less popular communication platform may exclude the people the organization is seeking to help.

The adoption of mobile messaging apps may also result in the Further Processing of collected data, including Personal Data. Mobile messaging apps make it possible to collect information online and may also provide new ways of analysing the available data. In other words, data and metadata collected via mobile messaging apps can help to triangulate information in new ways. In light of this and the probability of Further Processing of Personal Data, it is important to consider the purpose for using a messaging application as well as the entities with whom the collected data will be shared. Humanitarian Organizations may then find they are unable to state confidently that users can destroy or remove data already submitted, because this could entail multiple negotiations with multiple parties.

Mobile messaging apps were primarily designed to allow private communication between individuals or small groups. This type of functionality could be used by Humanitarian Organizations to provide basic counselling or to obtain information from beneficiaries about incidents, ongoing conflict or particular needs. However these apps may also be used in Humanitarian Action to "broadcast" content to large numbers of personal contacts or followers. In particular, in situations where the number of the users is very large, mobile messaging apps may work as a one-way broadcasting channel (e.g. to announce the time and place for delivery of humanitarian aid or changed opening hours of a local clinic).

11.1.1 Mobile messaging apps in Humanitarian Action

A messaging application (or app) is a software programme that allows users to send and receive information using their mobile phones or other smart portable devices. The ease with which apps work has had a great impact on their popularity, public acceptance and continuously increasing demand. There are three key differences between communication through mobile messaging apps and communication through mobile-phone networks:[174]

- Mobile messaging apps transmit and receive data using a Wi-Fi internet connection or a mobile data connection (unlike SMS messages, which are transmitted over conventional telephone networks).
- Mobile messaging apps can transmit or receive a much wider range of data types than is possible using SMS or even its multimedia-enabled successor, MMS. Mobile messaging apps have developed more similarities than differences over time and in addition to voice calls and text, messaging

173 See Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices (WP 202, 27 February 2013).

174 ICRC, The Engine Room and Block Party, *Humanitarian Futures for Messaging Apps* (January 2017): https://shop.icrc.org/humanitarian-futures-for-messaging-apps.html.

app users can also send and receive the following types of information: files, including photos, images and (in some cases) documents; audio recordings, including voice recordings that act in the same way as a voicemail message; data identifying their current location, based on their phone's GPS sensor; live video calls (in some apps); and emojis (pictographic representations of emotions or specific objects).
- Mobile messaging apps can transmit end-to-end encrypted content. They may, however, also generate and keep large amounts of – unencrypted – metadata.

Humanitarian Organizations have been adopting mobile messaging apps for reasons such as the following:[175]
- to target audiences (staff or beneficiaries) already using messaging apps;
- to reduce communications costs;
- to maintain reliable contact with people (whether staff or beneficiaries) in transit;
- to enable communication with people in environments where other communications methods are unavailable;
- to increase the speed of communications;
- to improve the security of digital communications as compared with existing methods of communication (where such apps offer end-to-end encryption of content);
- to facilitate information collection from or dissemination to hard-to-reach, remote or inaccessible areas;
- to speed up data collection or increase efficiency; and
- to improve inter-office coordination.

Based on the considerations above, there are two separate areas of analysis to be distinguished from a data protection point of view:
- Personal Data Processing through the mobile messaging apps themselves;
- Personal Data Processing by Humanitarian Organizations, of data collected through mobile messaging apps.

These are addressed, in turn, below.

11.2 Application of basic data protection principles

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

11.2.1 Processing of Persona Data through mobile messaging apps

Communicating with individuals affected by Humanitarian Emergencies through mobile apps requires Humanitarian Organizations, in most cases, to install and use applications already used by the majority of the population. Individuals, or in other words, beneficiaries in most cases have already downloaded and installed such applications and consented to their data protection terms.

By communicating with beneficiaries through mobile messaging apps, however, Humanitarian Organizations may suggest, whether directly or indirectly, that such means of communication are secure and that no harm is likely to arise for the beneficiaries in engaging with the Humanitarian Organization. It is important therefore, that, irrespective of the initial Consent given by the beneficiaries to the app provider to process their Personal Data, a clear analysis of the implications of such use is made by the Humanitarian Organization to ensure that no unexpected negative consequences are generated by their engagement. It is recommended to do this with a DPIA, which would take into account the

175 For a more detailed explanation of the reasons to adopt mobile messaging apps in Humanitarian Action, See *Humanitarian Futures for Messaging Apps*, ICRC, The Engine Room and Block Party, January 2017, *op.cit.*

considerations set out below. The outcome of the DPIA may be that only certain types of data can be collected or communicated through a particular app, or that a particular app may be used only in certain circumstances and not others. It may also be that the use of a particularly popular app may be inappropriate for the Humanitarian Organization, and that the Humanitarian Organization may want to use such an app only to notify individuals of its intention to communicate through another, more secure, app. In carrying out the assessment it is also important to note that messaging apps develop and change features fast, and there is no guarantee that a feature offered by an app will be available indefinitely. Similarly, companies' policies and statements about data usage, security and privacy may be revised at a later stage. Organizations will often be unable to view technical details of the underlying code, so they may be unable to make a comprehensive assessment of how any such changes affect users' security or privacy. Organizations that use third-party providers to manage or process information should also prepare to engage with these risks. Changes in app features may require revision of the DPIA.

The difference between one-way and two-way communication with beneficiaries through apps should also be highlighted, as the latter often carries much higher risks (potentially more Personal Data may be transferred) and also raises issues of long term management/sustainability against expectation.

11.2.1.1 Potential threats

Data protection and privacy concerns arise in every area of a Humanitarian Organization's work, so organizations should evaluate particular risks when considering whether to deploy a messaging app or not. Of these, the primary concern is the prospect that unintended Third Parties access data collected by Humanitarian Organizations, for purposes that run counter to the neutral, impartial and independent nature of humanitarian work (e.g. access by local authorities, law enforcement authorities, groups driven by various interests or private entities).

These Third Parties could include:

- entities in refugees' countries of origin, including armed groups and authorities, who may wish to identify groups or individuals for the purpose of harming and/or targeting them;
- entities with migration policy or security interests, who wish to understand and predict displacement trends and flows;
- entities with an interest in surveillance for national security purposes;
- hostile parties who wish to target Humanitarian Organizations and the people that they support and carry out violent attacks against them;
- commercial entities that wish to conduct behavioural profiling of particular groups, which can lead to discrimination.[176]

Concerns in this area have been acknowledged and supported by the International Conference of Privacy and Data Protection Commissioners, in its 2015 Resolution on Privacy and International Humanitarian Action:

> *"Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to Humanitarian Action more generally."*[177]

176 Maria Xynou and Chris Walker, *Why we still recommend Signal over WhatsApp*, 23 May 2016: https://securityinabox.org/en/blog/23-05-2016/why-we-still-recommend-signal-over-whatsapp.

177 International Conference of Data Protection and Privacy Commissioners, Adopted Resolutions, Resolution on Privacy and International Humanitarian Action, 2015: *op.cit.*

11.2.2 What kind of data do messaging apps collect or store?

Message content: Although some major messaging app companies state that their apps offer end-to-end encryption, meaning that they are unable to decrypt or read the contents of messages, other widely-used apps such as imo and Facebook Messenger store all message content on their servers. Note that some apps offering end-to-end encryption include it only as an opt-in feature (such as Telegram, LINE and Facebook Messenger). This means that unless users are aware of the need to enable this feature in their settings, all message data may still be sent unencrypted. Communication with most bots on services such as Telegram is not end-to-end encrypted.

User information: When users sign up for an app, they are asked to submit information about themselves (ranging from a phone number, in the case of most apps, to images, full names and email addresses in the case of apps such as WeChat and Facebook Messenger). Mandatory SIM card registration is enforced in many countries worldwide. In these countries, an app's requirement to submit a phone number may in effect prevent individuals from using messaging apps anonymously. In parts of Latin America, users may also be required to register their handset number.[178] Many apps automatically access a user's list of phone number contacts during sign-up to find other contacts that already have the app. In some cases, apps may store this data separately (WhatsApp, for example, confirmed in June 2016 that it stores contact list information).[179] Details of any groups to which the user belongs may also be stored in some cases.

Metadata: According to their terms of service, apps collect varying quantities of metadata, including sites and information accessed from within the app. Many app companies state that such data are retained on their servers, although they rarely clarify the length of time that data are retained, or if and how metadata are encrypted (even among apps that claim to have implemented end-to-end encryption). Although some messaging applications on personal computers offer to obscure users' metadata using Tor hidden services (software that enables anonymous browsing),[180] this is not an option on the major messaging apps currently available. Instead, the most privacy-conscious apps, such as Signal,[181] simply aim to collect as little metadata as possible.

Data shared with Third Party providers: Messaging app companies frequently state that they share users' Personal Data with other companies which provide services to enable the app to operate. However, they rarely state which companies they work with, what services they provide, what data they have access to, or how the data are processed and stored. Twilio, a third-party provider that works with some messaging app companies, provides limited transparency reports which indicate that it received 376 requests for data from international agencies in the first half of 2016 compared with 46 over the same period in 2015.[182]

Evidence that a user has installed an app on their phone: By accessing an individual's physical device, authorities could find physical evidence that a user has installed a particular messaging app. This could also potentially be accessed

178 GSMA, *Mandatory registration of prepaid SIM cards: Addressing challenges through best practice*, April 2016: www.gsma.com/publicpolicy/wp-content/uploads/2016/04/Mandatory-SIM-Registration.pdf.

179 Micah Lee, *Battle of the secure messaging apps: How Signal beats WhatsApp*, The Intercept, 22 June 2016: https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp/.

180 All the following use Tor hidden services (software that is designed to allow anonymous communication): Guardian Project, *What is Orbot?*: https://guardianproject.info/apps/orbot/; Security in a Box, *Guide to Orbot*, https://securityinabox.org/en/guide/orbot/android; *Tor Project, Tor Messenger Beta: Chat over Tor, Easily*, 29 October 2015: https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily; Joseph Cox, *'Ricochet,' the Messenger That Beats Metadata, Passes Security Audit,* 17 February 2016: http://motherboard.vice.com/read/ricochet-encrypted-messenger-tackles-metadata-problem-head-on.

181 Signal, *Grand jury subpoena for Signal user data*, Eastern District of Virginia, 4 October 2016: https://whispersystems.org/bigbrother/eastern-virginia-grand-jury/.

182 See Twilio, *Transparency Policy*: https://www.twilio.com/legal/transparency.

through other means – for example, users must associate an email address with their smartphone to download an app, creating a potentially traceable link between the app and other online activity.

11.2.3 How could other parties access data shared on messaging apps?

Other parties may be able to access data transmitted through messaging apps in a number of ways, including:

- A messaging app company (or a third-party provider that accesses app users' personal information) discloses message content or metadata that it stores on its servers, in response to a disclosure request from an authority in the jurisdiction where such data are stored.
- Another party gains unlawful or covert access to message content or metadata stored on a messaging app company's servers (through hacking) or accesses that information while it is travelling between the two actors (known as a "man-in-the-middle" attack). For example, tests by the University of Toronto's Citizen Lab in late 2013 indicated that the messaging app LINE was not encrypting content sent over 3G connections despite the fact that content sent over Wi-Fi was encrypted.[183]
- Parties access messaging app content through other covert methods. These include accessing the SMS login codes sent to users when they sign up for an app by redirecting traffic on conventional mobile phone networks,[184] or inducing users to install "malware" (short for malicious software) onto their phone which enables others to remotely gain access to that phone or data stored on it.[185]
- An individual is forced to hand over their physical device. End-to-end encryption only encrypts data in transit, not on the user's device. If a party gains physical access to a phone or computer with access to a user's messaging apps account (such as by compelling the user to unlock it), they may be able to access message content as well as details of apps that are installed on the device. In some countries, authorities consider merely installing apps such as WhatsApp as an indicator of subversive behaviour.[186] Signal, Telegram and SnapChat all offer "self-destructing messages", which are only visible on the sender and recipients' phones for a limited time before being automatically deleted.
- A messaging app company allows an authority to directly access content or data transmitted over the app by building a secret feature into its code (known as a "backdoor"). For example, certain countries have reportedly threatened to fine messaging app companies that did not introduce backdoors into their code, specifically citing WhatsApp, Telegram and Viber.[187] Other companies have publicly stated that that they have refused requests from government agencies to create backdoors.[188]

183 3G networks are encrypted by default, but only at the level of the network provider, meaning that internet service providers (ISPs) and telecommunications companies can decrypt information sent over them. Citizen Lab, *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*, November 2013: https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications/; Jon Russell, *Thailand's Government Claims It Can Monitor The Country's 30M Line Users*: https://techcrunch.com/2014/12/23/thailand-line-monitoring-claim/.

184 Frederic Jacobs, *How Russia Works on Intercepting Messaging Apps*, 30 April 2016: https://www.bellingcat.com/news/2016/04/30/russia-telegram-hack/; Operational Telegram, 18 November 2015: https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a#.f1vg48cl1.

185 See for example, Iran Threats, *Malware posing as human rights organizations targeting Iranians, foreign policy institutions and Middle Eastern countries*, 1 September 2016: https://iranthreats.github.io/resources/human-rights-impersonation-malware/.

186 Electronic Frontier Foundation, *Your Apps, Please? China Shows how Surveillance Leads to Intimidation and Software Censorship*, January 2016: https://www.eff.org/deeplinks/2016/01/china-shows-how-backdoors-lead-software-censorship; Maria Xynou and Chris Walker, *Why we still recommend Signal over WhatsApp*, 23 May 2016: https://securityinabox.org/en/blog/23-05-2016/why-we-still-recommend-signal-over-whatsapp.

187 Patrick Howell O'Neill, *Russian bill requires encryption backdoors in all messenger apps*, 20 June 2016: http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb/.

188 Jon Russell, *Tim Cook Says Apple Won't Create Universal iPhone Backdoor For FBI*, 17 February 2016, https://techcrunch.com/2016/02/17/tim-cook-apple-wont-create-backdoor-to-unlock-san-bernardino-attackers-iphone/; Max Eddy, *What It's Like When The FBI Asks You To Backdoor Your Software*, 8 January 2014: http://securitywatch.pcmag.com/security/319544-what-it-s-like-when-the-fbi-asks-you-to-backdoor-your-software.

11.2.4 Messaging app features related to privacy and security

The following are relevant features to look for when choosing a messaging app to exchange information in humanitarian situations.

11.2.4.1 Anonymity permitted/no requirement for authenticated identity

Enabling users to communicate anonymously via a messaging app enhances their privacy, whereas requiring the use of real names, email addresses and authenticated identities increases the risk that individuals will be monitored or targeted. The less information a user is required to provide in order to use an app, the less information about them other parties may be able to access.

11.2.4.2 No retention of message content

User privacy is better served when the contents of messages are delivered to a user's device and deleted from the app company's servers after they are read. Apps such as Telegram, WhatsApp, Viber and Signal state that they delete message content from their servers immediately after the intended recipient has accessed it. However, companies such as Skype retain message content on their servers after the user has read the message, without stating a maximum time limit after which they will delete the data.

11.2.4.3 End-to-end encryption

End-to-end encryption restricts the ability of Third Parties such as governments or adversaries to intercept communications between Humanitarian Organizations and their beneficiaries in a way that allows the message contents to be viewed. In this case, even if a company does retain content data, this will be in encrypted form and thus not legible to the company or to any Third Party seeking access to the data. Encryption thus restricts the type and amount of legible data that messaging-app companies can be compelled to disclose. Ideally, it should be deployed by default in both one-to-one and group chats. There are online resources which assess the levels of security offered by specific apps.[189]

11.2.4.4 User ownership of data

It is essential that messaging-app users be regarded as the lawful owners of their personally identifiable data as well as the contents of their messages. This prevents messaging-app companies from using such data for commercial or other purposes without the explicit Consent of the user. This issue is addressed by national law in some countries and the topic may also be included in the messaging apps' terms-of-service agreements.

11.2.4.5 No or minimal retention of metadata

The less metadata messaging apps retain on their servers, the less data they can be compelled to disclose to governments or sell to commercial interests. Messaging apps such as Signal and Telegram claim not to retain any metadata on their users, although Telegram's claim is contested,[190] whereas most major apps under consideration state that they collect contact numbers, logs of activity on the app and location information.

11.2.4.6 Messaging-app code is open source

When the code which underpins a messaging app is open source, the app can be independently scrutinized to verify that it has no vulnerabilities to security threats or hidden surveillance functions such as backdoors. Ideally, an app will publish its entire codebase openly: messaging apps such Signal and Wire are entirely open source, while apps such as Telegram and Threema publish only part of their code.[191]

189 Electronic Frontier Foundation, Secure Messaging Scorecard: https://www.eff.org/secure-messaging-scorecard.

190 Jeremy Seth Davis, *Telegram metadata allows for 'stalking anyone'*, 30 July 2015: http://www.scmagazine.com/telegram-metadata-allows-for-stalking-anyone/article/456484/.

191 For more on this topic, see Lorenzo Franceschi-Bicchierai, *Wickr: Can the Snapchat for Grown-Ups Save You From Spies?*, 4 March 2013: http://mashable.com/2013/03/04/wickr/#3EwYsDKZ5kqh.

11.2.4.7 Company vets disclosure requests from law enforcement

It is critical that the company producing the messaging app rigorously vets and responds in a restrained manner to law-enforcement requests for user data. Ideally, they will provide information on their own behaviour in this regard, publishing regularly updated transparency reports that provide details about what requests they have received from which jurisdictions, and what types of information they have provided. At the time of writing, Microsoft[192] and Facebook[193] publish regular transparency reports that detail how many requests they receive and how much data they hand over to law-enforcement agencies, while Open Whisper Systems (the company behind Signal) provides more detailed descriptions of the small number of requests they receive.[194]

Additionally, it is important to consider whether an entity providing a messaging app is located in a country where the government has broad surveillance powers or a record of regularly flouting legal restraints on surveillance.[195]

11.2.4.8 Limited Personal Data sharing with Third Parties

Although messaging apps will need to share some data with Third Parties (typically those playing some technical role in the data Processing) in order to facilitate the delivery of their services, it is critical that companies do not share Personal Data, and only share data that have been minimally de-identified when this is strictly necessary. Organizations should choose a messaging app that does not share any data with Third Parties other than that which is strictly necessary for the technical operation of the service – and seek to confirm this explicitly with companies before proceeding.

11.2.5 Processing of Personal Data collected through mobile messaging apps

Once the beneficiaries engage in communications with Humanitarian Organizations through mobile messaging apps, Humanitarian Organizations will need to collect, most likely store on other platforms, aggregate and analyse the information provided.

It is key that this Processing also takes place in line with the data protection principles set out in Part I of this Handbook. A few selected principles, specific to the collection of data through mobile messaging apps, are considered below.

Communicating with communities in humanitarian situations always involves negotiating a range of complex questions, including:

- Do individuals need to give a Humanitarian Organization "permission" to add their details to a group or channel?
- How can an individual opt out of receiving the content? Is this made clear to them at the outset?
- How can people be made aware of who their Personal Data are shared with?
- If requests for support that fall outside the Humanitarian Organization's mandate are shared with another humanitarian agency, are there clear data-sharing protocols to cover this?
- How do people know how long their data will be kept, and for what purposes?
- How can all these issues be communicated in a way that is easy to understand, including for people with limited experience of technology?

Working with messaging apps adds a new layer of complexity to all these issues.

192 Microsoft Transparency Hub: https://www.microsoft.com/about/csr/transparencyhub/.
193 Facebook, Government Requests to Facebook: https://govtrequests.facebook.com/about/.
194 Open Whisper Systems, Government Requests: https://whispersystems.org/bigbrother.
195 Useful sources for further research include: https://www.digcit.org/; https://privacyinternational.org/global-advocacy; https://advox.globalvoices.org/; and https://www.eff.org/deeplinks.

11.3 Legal bases for Personal Data Processing

Humanitarian Organizations may process Personal Data collected through mobile messaging apps using one or more of the following legal bases:[196]

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

In most cases, the Processing of Personal Data collected through mobile messaging apps may be based on Consent, vital interest or the public interest. If individuals have already communicated with a Humanitarian Organization by messaging app, or have given their telephone numbers to them, then Consent to receive messages can be assumed. Consent, however, must be informed, and it is key that Humanitarian Organizations provide the relevant information concerning the purpose, retention or further sharing of collected data, etc. as discussed in the relevant Section of this Handbook.[197]

Otherwise, messages concerning Humanitarian Emergencies can be assumed to fall within the vital interest of Data Subjects or to be in the public interest. These legal bases also require that information be given to individuals, which can be done by sending them a link to the relevant information notice in a message via the mobile messaging application used.

11.4 Data retention

Humanitarian Organizations need to set out in their information notices and data protection policies how long they envisage holding the data collected.

Some of the data entered into most messaging apps are retained and stored by Third Parties (messaging app companies), which in turn share some of that data with other parties – whether service providers that enable an app to function, or parent companies (as with Facebook and WhatsApp). It is therefore also worth pointing out in the Humanitarian Organization's information notice that the data provided through the app will also be retained by the app provider and any Third Parties involved, under the responsibility of the app provider and governed by their data protection policies.

Humanitarian Organizations should also consider having a retention policy concerning the exchanges of information or "chats" themselves and delete the chat history at regular intervals to ensure data minimization.

11.5 Data Subject Rights to rectification and deletion

As per Part I of this Handbook, Humanitarian Organizations should provide for mechanisms to facilitate the effective exercise of Data Subjects' rights, and inform Data Subjects thereof, in their data protection policies.

While this may be not problematic with regard to the data extracted from the messaging apps by the Humanitarian Organizations, it may be difficult to state confidently that messaging apps allow users to destroy or remove data that they have already submitted, because this could entail negotiations with multiple parties (not all of whom are transparent about the data that they hold). It is recommended that this factor also be specified in the data protection policy.

196 See Chapter 3: Legal bases for Personal Data Processing.
197 See Chapter 2: Basic principles of data protection.

11.6 Data Minimization

Considering the limited control Humanitarian Organizations have with regard to data collection by mobile messaging apps, organizations seeking to use messaging apps should aim to minimize the amount of information that is submitted to them. Academic research focused on the US has also found that users of messaging apps are usually unaware of the privacy implications of installing and sharing data on messaging apps.[198] Therefore, it is suggested that Humanitarian Organizations should provide incentives for crisis-affected individuals to share Personal Data that are strictly necessary to provide humanitarian aid.

EXAMPLE:

Ahead of South Africa's municipal elections in August 2016, the non-profit Africa's Voices Foundation partnered with Livity Africa to evaluate the impact of Voting is Power, a campaign to encourage young people to vote and highlight issues that mattered to them.[199]

To do so, they used online surveys of young people (conducted via email and through WhatsApp and Facebook Messenger) and posts published on social media. WhatsApp and Messenger were selected as channels because of their popularity with young people (476 people were engaged through Facebook Messenger and 46 through WhatsApp). Africa's Voices Foundation felt that their use of WhatsApp groups encouraged conversations that would yield particularly useful feedback. Impact and Communications Officer Rainbow Wilcox said: "the data that can be gathered [through WhatsApp] is rich, authentic, and provides insights into sociocultural beliefs and behaviours."

However, Africa's Voices had concerns about privacy when using both Facebook Messenger and WhatsApp. "We sought informed consent and stored the data securely, but we cannot control how the data will be used in these platforms," Claudia Abreu Lopes, Head of Research and Innovation, said. "It was problematic because we asked for personal information such as voting and demographics. We have decided not to embark on a [similar] project again if the privacy risks are not well understood before it starts."

As suggested above, it is recommended that Humanitarian Organizations also consider having clear policies on deleting chats at regular intervals, once the necessary data have been extracted.

11.7 Purpose limitation and Further Processing

In most cases data collected through mobile messaging apps will be extracted and analysed by Humanitarian Organizations on other platforms. As part of the Humanitarian Organizations' data protection policies to be communicated to the Data Subjects, Humanitarian Organizations should also clearly specify the purpose of Processing.

This can be particularly challenging considering the flexibility of use and immediacy of communication offered by such solutions, as it is likely that in any one chat numerous issues will be raised by a Data Subject, with each issue requiring one or more follow-up actions. With this in mind, and considering the compatibility of humanitarian purposes, it is suggested that a general humanitarian assistance and protection purpose specification should suffice.

Again, as Processing by mobile messaging applications is beyond the control of Humanitarian Organizations, the fact that such applications may process data for different purposes, according to their own data protection policies, should also be mentioned in the Humanitarian Organization's data protection policy.

198 Kelley P.G., Consolvo S., Cranor L.F., Jung J., Sadeh N., Wetherall D. (2012) *A Conundrum of Permissions: Installing Applications on an Android Smartphone*. In: Blyth J., Dietrich S., Camp L.J. (eds) Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science, vol 7398. Springer, Berlin, Heidelberg: http://dx.doi.org/10.1007%2F978-3-642-34638-5_6.

199 Africa's Voices, Case Study: Livity South Africa: http://www.africasvoices.org/case-studies/livity-south-africa/.

11.8 Managing, analysing and verifying data

Making use of data processed through messaging apps in Humanitarian Action is a challenge. Greater numbers of people can now collect and share larger volumes of data with organizations, but this means the organizations need to ensure they have the capacity to manage, analyse and verify collected data.

Difficulties can arise in creating a workflow to manage and analyse the information received. The systems used by messaging apps are not interoperable with existing information-management systems or databases; manual transcription of individual messages into spreadsheets is often the only way to allow Humanitarian Organizations to analyse data in a way that would allow for effective decision-making.

Challenges also arise with regard to verifying information received through messaging apps. While this is an issue in many online channels,[200] verifying content from messaging apps is made more challenging by the speed at which information can be sent, as well as by message volume and the range of data types that can be sent. News media and human-rights defenders have attempted to respond to these challenges through collaboration and efforts to produce resources and guidance on the issue. Some of these resources may also be useful to Humanitarian Organizations.[201]

Humanitarian Organizations engage in Further Processing in cases where the Personal Data collected via apps are managed, analysed or verified. Consequently, Humanitarian Organizations have to ensure that Further Processing of Personal Data operations is compatible with the initial purpose for which data was collected.

11.9 Data protection by design

If Humanitarian Organizations intend to develop a messaging app, they should consider implementing the principle of data protection by design, which requires the development of privacy-friendly systems and services both for technical solutions and organizational measures. Carrying out a Data Protection Impact Assessment (DPIA) is a way to implement the principle of data protection by design in practice. The client-server architecture used to store data should also give effect to the principle of data protection by design.

200 The Engine Room, *Verification of social media: The case of UNHCR on Twitter:* https://responsibledata.io/reflection-stories/social-media-verification/.

201 See for example, Craig Silverman (ed.), *The Verification Handbook,* European Journalism Centre, http://verificationhandbook.com/; Various authors, DatNav: *New Guide to navigate and integrate digital data in human rights research,* The Engine Room, Benetech and, Amnesty International, 2016; https://www.theengineroom.org/datnav-digital-data-in-human-rights-research/; First Draft News Partner Network, https://firstdraftnews.com/partners-network/.

Appendix I:

TEMPLATE FOR A DPIA REPORT

Cover page

- Data Protection Impact Assessment on [name of activity];
- Contact person, title and email address; and
- Date

Executive summary

If the DPIA is more than 20 pages, it should include an executive summary. The executive summary should include details of why the DPIA was undertaken, for whom and who conducted it. The executive summary should include the key findings and principal recommendations.

Introduction and overview of the DPIA process

The introduction should outline the scope of the DPIA, when, why and for whom it was performed and by whom. It should provide some information about the activity assessed. It should introduce the methodology employed in the DPIA (e.g. the method chosen to engage stakeholders).

Threshold assessment

This section should list the questions addressed by the Humanitarian Organization to determine whether a DPIA was necessary and what should be the scale of the DPIA.

Description of the activity or project to be assessed

The description of the activity to be assessed should state who is undertaking the activity and when it is to be undertaken. It should state who will be affected by the activity, who might be interested in or affected by the activity. The description should provide contextual information about how the activity fits in with the Humanitarian Organization's other services or activities.

Information flows

This section should detail (at a minimum):

- the type of data to be collected;
- whether sensitive information will be collected;
- how the data will be collected;
- for what purposes the data will be used;
- how and where the data will be stored and/or backed up;
- who will have access to the Personal Data;
- whether Personal Data will be disclosed;
- whether sensitive Personal Data will be disclosed; and
- whether any data will be transferred to other organizations or countries.

Compliance with laws, regulations, codes and guidelines

The DPIA report should identify the laws, regulations, codes of conduct and guidelines with which the activity complies or should comply. At the global level, the privacy principles listed in the ISO/IEC 29100:2011 standard of the International Organization for Standardization (ISO)[202] are useful as a reference in a DPIA. In addition, the DPIA report should state how it complies with the Humanitarian Organization's confidentiality rules and codes of conduct, and how the Humanitarian Organization monitors compliance.

Stakeholder analysis

The report should identify who are the principal stakeholders interested in or affected by the data Processing and how the DPIA or the Humanitarian Organization arrived at this list.

202 https://www.iso.org/standard/45123.html

Data protection impacts (risks)

This section should detail the privacy risks identified in relation to the main privacy principles found in relevant legislation and the Humanitarian Organization's confidentiality rules and codes of conduct.

Risk assessment

This section of the report should include details of how the risks were assessed and the results of any risk assessment undertaken.

Organizational issues

The DPIA report should include a section that describes how senior management is involved in decision-making related to data protection. This should include discussion identifying any organizational issues that are directly or indirectly affected by the data Processing activity. For example, it may become apparent that the data Processing requires putting in place an organizational mechanism for ensuring accountability, i.e. that a senior manager is responsible for ensuring that the programme does not negatively affect the Humanitarian Organization or its stakeholders.

In the course of the DPIA, it may become apparent to the DPIA team that the Humanitarian Organization needs to spend more time on raising the awareness of employees about privacy and/or ethical issues, and that the Humanitarian Organization needs to mainstream data protection in the organization. The report should state what the Humanitarian Organization does now to raise employee awareness of data protection and how it could improve.

The report should state how the Humanitarian Organization identifies, investigates and responds to data protection incidents, e.g. data protection breaches, how the Humanitarian Organization decides to notify affected parties and how it seeks to learn from an incident.

This section should also describe how the Humanitarian Organization responds to requests for access to personal information or to correct or amend the information it has gathered and to whom the data are transferred and what safeguards the Humanitarian Organization insists be in place before making a transfer.

Results of the consultation(s)

The report should specify what efforts the Humanitarian Organization has made to consult with stakeholders, to gather their views and ideas about potential data protection impacts, how they might be affected by the data Processing (positively and/or negatively) and how negative impacts could be mitigated, avoided, minimized, eliminated, transferred or accepted.

The DPIA team should specify which consultation techniques were employed (surveys, interviews, focus groups, workshops, etc.), when they were undertaken, the results of each consultation exercise, and whether differences in opinion were discovered when different techniques were used.

The DPIA should state who was consulted and what information materials the Humanitarian Organization provided to stakeholders, including families of the missing.

The DPIA should state whether the consultations yielded any new findings and what efforts the Humanitarian Organization had made to take into account stakeholder views and ideas in the design of the data Processing activity.

Recommendations

The DPIA team should set out their recommendations for avoiding, minimizing, transferring or sharing the data protection risks. Some risks may be worth taking and, if so, the DPIA should say why. The DPIA should be clear who will bear the risk (i.e. will it be the Humanitarian Organization or stakeholders or others?). The DPIA should also set out what further work is necessary or desirable to implement its recommendations (for example, the DPIA should mention the need for independent third-party monitoring of its recommendations.

The DPIA should also make recommendations as to whether the DPIA report should be made public. There may be circumstances where it might not be appropriate to make the DPIA or parts of it public – e.g. there may be confidentiality or security reasons. Often the report can be redacted in places and then made public or sensitive parts can be placed in a confidential appendix. Alternatively, the Humanitarian Organization could provide a summary of the DPIA report.

Appendix II:
WORKSHOP PARTICIPANTS

Workshop organizers

FIRST NAME	LAST NAME	Organization
LINA	JASMONTAITE	Brussels Privacy Hub
IOULIA	KONSTANTINOU	Brussels Privacy Hub
CHRISTOPHER	KUNER	Brussels Privacy Hub
VAGELIS	PAPAKONSTANTINOU	Brussels Privacy Hub
AMY	WEATHERBURN	Brussels Privacy Hub
PIERRE	APRAXINE	International Committee of the Red Cross
ROMAIN	BIRCHER	International Committee of the Red Cross
VICTORIEN	HANCHÉ	International Committee of the Red Cross
MASSIMO	MARELLI	International Committee of the Red Cross

Workshop participants

FIRST NAME	LAST NAME	Organization
KRISTINE	BEHM	Barclays
JOËLLE	JOURET	Belgian Privacy Commission
ISABELLE	MOELLER	Biometrics Institute
GLORIA	GONZALEZ FUSTER	Brussels Privacy Hub
ERICA	SEE	Canadian Red Cross
ISABELLE	PELLY	Cash Learning
VICTOR	HOLLEBOOM	Council of Europe
SOPHIE	KWASNY	Council of Europe
CHRISTINA	STRÖMHOLM	Council of the EU
SARAH	GALAU	Doctors Without Borders
RODOLPHE	MUNOZ	EFTA Surveillance Authority
TOM	WALKER	Engine Room
ANDREA	DAMINI	European Commission, DG ECHO
MANUEL	GARCIA SANCHEZ	European Commission, DG Justice
ALBA	BOSCH MOLINE	European Data Protection Supervisor

ISABELLE	CHATELIER	European Data Protection Supervisor
MARIO	GUGLIELMETTI	European Data Protection Supervisor
ROMAIN	ROBERT	European Data Protection Supervisor
RUDY	VAN DEN BERGH	European UAV-Drones Area
TARITHA	SARI	Fairphone
FLORIANE	LECLERCQ	French-speaking Association of Personal Data Protection Authorities
JOSH	LYONS	Human Rights Watch
KARS	AZNAVOUR	International Committee of the Red Cross
MARIA ELENA	CICCOLINI	International Committee of the Red Cross
ANDRE	DUERR	International Committee of the Red Cross
NATACHA	FARINA GROUX	International Committee of the Red Cross
DANIEL	FUEGER	International Committee of the Red Cross
VINCENT	GRAF	International Committee of the Red Cross
LAUREN	HERBY	International Committee of the Red Cross
JULES	KAGWAHABI AMOTI	International Committee of the Red Cross
JACOBO	QUINTANILLA	International Committee of the Red Cross
SYLVAIN	VITE	International Committee of the Red Cross
CLAIRE	DUNHAM	International Federation of the Red Cross
LESLIE	HASKELL	International Federation of the Red Cross
LUCIE	LAPLANTE	International Federation of the Red Cross
HEATHER	LESON	International Federation of the Red Cross

CHRISTINE	ADAM	International Organization for Migration
JOSEPH	ASHMORE	International Organization for Migration
CHRISTINA	VASALA KOKKINAKI	International Organization for Migration
CAROLINE	LOUVEAUX	MasterCard
LILY	FREY	Mercy Corps
KATE	KRUKIEL	Microsoft
JOHNY	GASSER	Orange Business Services
BEN	HAYES	Privacy Consultant
TOM	FISHER	Privacy International
ALEXANDRINE	PIRLOT DE CORBION	Privacy International
CINDY	BIRMANN	Royal Military Academy Belgium
MARC	BURGGRAEVE	Royal Military Academy Belgium
BENOIT	UFFER	Sensometrix
ANDRÉS	CALVO MEDINA	Spanish Data Protection Agency
RAFAEL	GARCIA GOZALO	Spanish Data Protection Agency
PIERRE-YVES	BAUMANN	Swiss Data Protection Authority
CATHERINE	LENNMAN	Swiss Data Protection Authority
BRYAN	FORD	Swiss Federal Institute of Technology in Lausanne

MILA	ROMANOFF	UN Global Pulse
JOE	CANNATACI	UN Special Rapporteur on the Right to Privacy
CAROLINE	DULIN BRASS	United Nations High Commissioner for Refugees
JOANNA	FRIEDMAN	United Nations High Commissioner for Refugees
ANDREW	HOPKINS	United Nations High Commissioner for Refugees
YANYA	VISKOVICH	United Nations High Commissioner for Refugees
LOUISE	GENTZEL	United Nations Office for the Coordination of Humanitarian Affairs
MARK	MCCARTHY	United Nations Office for the Coordination of Humanitarian Affairs
MAYA	HERTIG	University of Geneva
ROB	DE ROO	VIVES University College
ARAMAIS	ALOJANTS	World Food Programme
MAURIZIO	BENEDETTI	World Food Programme
YOSHIKO	MAKINO	World Food Programme
JACQUELINE	STEIN-KAEMPFE	World Food Programme
EDGARDO	YU	World Food Programme
LES	CUTTER	World Vision International

MISSION

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

ICRC

ISBN 978-2-940396-56-6

4305/002 09.2017 1000