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.[1]

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 are subject to the control of and enforcement by their own compliance systems.[2] Thus, they constitute their own "jurisdiction", and data flows within them, for example between HQ and field locations or between field locations, and between them and their subordinate bodies, do not fall within the scope of this chapter.[3]

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

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

1 See Chapter 10: Cloud Services.

2 Massimo Marelli, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", *Computer Law and Security Review*, Vol. 50, 2023, 105849: https://doi.org/10.1016/j.clsr.2023.105849.

3 See Section 2.4 – Applicable law and International Organizations.

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

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

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

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

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.[4] 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[5] (including any data protection or privacy requirements of local law, if applicable) have been satisfied prior to the transfer.
- A legal basis must be provided for the transfer.
- An assessment should be carried out to determine whether the transfer presents any unacceptable risks for the individual (e.g. discrimination or repression).

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

5 See Chapter 2: Basic principles of data protection.

- The organization that initiates the transfer must be able to demonstrate that adequate measures have been undertaken to ensure compliance with the data protection principles set forth in this Handbook by the recipient entity in order to maintain the level of protection of Personal Data with regard to International Data Sharing (accountability).
- The individual should be informed about the recipient(s) of the transfer. The transfer should not be incompatible with the reasonable expectations of the individuals whose data are transferred.

4.3 PROVIDING A LEGAL BASIS FOR INTERNATIONAL DATA SHARING

4.3.1 INTRODUCTION

As mentioned above, this Handbook is designed to assist in the application and respect of data protection principles and rights in humanitarian situations. It does not, however, replace or provide advice on domestic legislation on data protection, where such applies to a Humanitarian Organization that does not benefit 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, insofar 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 Data Protection Officer (DPO), legal department and/or local legal adviser.

4.3.2 LEGAL BASES FOR INTERNATIONAL DATA SHARING

International Data Sharing may be carried out:

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

These legal bases are used in similar ways to their application in Personal Data Processing.[6] In addition, as International Data Sharing involves additional risks, the factors listed below in Section 4.4 – Mitigating the risks to the individual should be given due consideration.

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

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, or is an international organization, 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.

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/ Contractual clauses, 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 European Union/European Economic Area[7] 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[8] 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.
- The data are being processed on the basis that they are protected by an International 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

7 See European Commission, "Standard Contractual Clauses for Data Transfers between EU and Non-EU Countries", Text, European Commission – European Commission, 4 June 2021: commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

8 See for example: International Conference of the Red Cross Red Crescent Movement, "Restoring Family Links Code of Conduct on Data Protection", 18 January 2016: www.icrc.org/en/document/rfl-code-conduct.

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. The NGO also has a record of losing data that is sent to it. The Humanitarian Organization should seriously consider not transferring the data, irrespective of contractual clauses being signed.

To identify and address or mitigate such risks properly, a DPIA should be carried out.[9] In case of doubt, the Humanitarian Organization's DPO should be consulted.

4.4.2 ACCOUNTABILITY

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

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

For any International Data Sharing, appropriate measures should be used to safeguard the transmission of Personal Data to Third Parties. The level of security[10] adopted and the method of transmission should be proportionate to the nature and sensitivity of Personal Data and to the risks involved. It is also advisable to consider this factor as part of any DPIA to further specify the precautions to be taken.

4.5 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

In the event that a Data Processor is employed by a Data Controller, irrespective of whether the Data Processor is located in a country other than that of the establishment of the Data Controller, their relationship should as much as possible be

9 See Chapter 5: Data Protection Impact Assessments (DPIAs).

10 See Section 2.8 – Data security and Processing security.

governed by a binding agreement to protect the Processing of the Personal Data that are shared between them.

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

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