CHAPTER 2

BASIC PRINCIPLES OF DATA PROTECTION

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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.[1]

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 affected populations 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 a teleological interpretation of rights,[2] i.e. one that prioritizes the purposes the rights serve.

EXAMPLE:
Data protection law requires that individuals be given basic information about the Processing of their Personal Data. However, in a Humanitarian Emergency it is necessary to balance this right against other rights, and in particular the rights of all affected individuals. It would therefore not be necessary to inform all individuals of the conditions of data collection prior to receiving aid, if this would seriously hamper, delay or prevent the distribution of aid. Rather, the Humanitarian

1 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.

2 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.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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.[3] 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.[4]

The boxed checklist 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?

3 See ICRC, "ICRC WWI Prisoner Archives Join UNESCO Memory of the World", 15 November 2007: www.icrc.org/en/doc/resources/documents/feature/2007/ww1-feature-151107.htm.

4 See Els Debuf, "Tools to do the job: The ICRC's legal status, privileges and immunities', *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015, pp. 319–344: https://doi.org/10.1017/S181638311500051X.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

- 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[5]

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

Processing means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

the aerial imagery (subject to the resolution and other factors potentially making it possible to identify individuals) is not by itself Personal Data, but such data can be extremely sensitive in certain circumstances. The Humanitarian Organization should have protected this data and not revealed it.

It is also important to understand the distinction between **Data Controller** and **Data Processor**. A Data Controller is the person or organization who alone or jointly with others determines the purposes and means of the Processing of Personal Data, whereas a Data Processor is the person or organization who processes Personal Data on behalf of the Data Controller. Finally, a Third Party is any natural or legal person, public authority, agency, or any entity 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 non-governmental organization (NGO) to help deliver the aid, which needs to use the identification information originally collected by the Humanitarian Organization. The two organizations sign a contract governing the use of the data, under which the International Humanitarian Organization has the power to direct how the NGO uses the data and the NGO commits to respect the data protection safeguards required by the Humanitarian Organization. The NGO also engages an IT consulting company in order to perform routine maintenance on its IT system in which the data are stored.

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

2.3 AGGREGATE, PSEUDONYMIZED AND ANONYMIZED DATA SETS

As mentioned above, it is outside the scope of this Handbook to discuss the Processing of data that does not relate to individual persons, such as data that have been rendered anonymous in such a way that a Data Subject is no longer identifiable.

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,

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

including sharing and/or publication, of such data cannot lead to the Reidentification of individuals.[6]

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 aiming to anonymize data, it is essential to ensure that data sets containing Personal Data are fully and *irreversibly* anonymized, i.e. that Reidentification is not possible. Anonymization processes are challenging, especially where large data sets containing a wide range of Personal Data are concerned and may pose a greater risk of Reidentification.[7]

"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[8] data in a data set with a number. Sharing registration/identification numbers instead of names is good practice, but does not amount to Anonymization.

The application of Pseudonymization to personal data can reduce the risks to the Data Subjects concerned by reducing the likelihood that they will be reidentified. The term "Reidentification" describes the process of turning allegedly anonymized or pseudonymized data back into Personal Data through the use of data matching or similar techniques.[9] Pseudonymization can also help controllers and processors meet their data protection obligations. Nevertheless, not every Pseudonymization technique fulfils data protection requirements on its own, and Pseudonymization techniques that may work in one specific case may not be sufficient to protect Personal Data in other cases.[10]

6 See UK Statistics Authority, *National Statistician's Guidance: Confidentiality of Official Statistics – GSS*, accessed 6 January 2022: https://gss.civilservice.gov.uk/policy-store/national-statisticians-guidance-confidentiality-of-official-statistics.

7 See UK Information Commissioner's Office (ICO), *Anonymisation: Managing Data Protection Risk Code of Practice*, ICO, Wilmslow, Cheshire, November 2012: https://ico.org.uk/media/1061/anonymisation-code.pdf.; see also EU Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

8 "Anagraphic", in *Wiktionary*, 14 November 2020: https://en.wiktionary.org/w/index.php?title=anagraphic&oldid=61117548.

9 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.

10 See: Athena Bourka and Prokopios Drogkaris, eds., *Data Pseudonymisation: Advanced Techniques and Use Cases*, European Union Agency for Cybersecurity (ENISA), 28 January 2021: www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

Data protection principles have to be applied carefully when assessing these techniques, and risk analysis tools have to be apt to evaluate whether the mitigation techniques applied are effective. Principles such as purpose limitation and retention are of particular importance here, as they can help ensure that existing pseudonymized databases are not repurposed for new projects or combined with newer ones. Additionally, there will always be a trade-off between adding confidentiality to a data set and reducing its utility. Many privacy-preserving techniques work by perturbing (i.e. altering or obfuscating) the data to be released, resulting in data that, depending on scope, might be less useful for the purposes of the sharing or research.[11]

Prior to sharing or publicizing anonymized data, it is important to ensure that no Personal Data are included in the data set and that individuals cannot be re-identified. If the risk of Reidentification 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 Reidentification with absolute certainty. Generally speaking, Reidentification becomes significantly more likely where no mitigation measure is taken to protect Personal Data. This can be possible, for instance, where an entity holds certain data sets concerning the affected populations, which can then be combined with the Processed Data to generate new information about Data Subjects or the groups to which they belong.

For example, 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, such as by mapping data like 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 NGOs subject to the jurisdiction of the country in which they operate, while others are International Organizations with privileges and immunities allowing them to perform the mandate attributed them by the community of states under international law in full independence.

11 Gregory J. Matthews and Ofer Harel, "Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy", *Statistics Surveys*, Vol. 5, 1 January 2011, pp. 1–29: https://doi.org/10.1214/11-SS074.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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).[12]

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

International Organizations enjoy privileges and immunities, in particular, 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".[13] 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

12 See Section 1.2 – Objective.

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

2.5.2 THE PURPOSE LIMITATION PRINCIPLE

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

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

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

2.5.2.1 FURTHER PROCESSING

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

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

- the link between the initial purpose(s) and the purpose(s) of the intended Further Processing;

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

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

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

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

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

Examples of circumstances in which Further Processing may be considered incompatible include cases where the Personal Data have been collected as part of the information necessary to assist in the tracing of a Sought Person. Processing this

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

information further in order to request that the relevant authorities carry out an investigation into the possible violations of the applicable law (for example, in the context of civilian population protection activities) may not be compatible as Further Processing. This is due to the possible detrimental consequences of the intended Further Processing for Data Subjects and the likely difficulty of providing appropriate safeguards.

Should the intended purpose of Further Processing not be compatible with the purpose for which the data were initially collected, the data should not be further processed, unless it is deemed appropriate to do so under another legal basis. In this case, additional measures may be required depending on the basis that applies.[14]

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, and make the Further Processing compatible.

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

2.5.3 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

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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.[15]

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 affected people. Humanitarian Organizations also need to weigh their need for data against the potential harm to individuals of such data being collected, as well as the risk of "assessment fatigue" and potentially raising unrealistic expectations among the people they seek to help.

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

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

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

15 See Section 2.7 – Data retention.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

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

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

2.5.5 THE PRINCIPLE OF DATA QUALITY

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

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

2.6 SPECIAL DATA PROCESSING SITUATIONS

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

2.6.1 HEALTH PURPOSES

Improper handling (including disclosure) of Health Data could cause significant harm to the individuals concerned. Accordingly, Health Data should be considered as particularly sensitive and specific guarantees should be implemented when Processing such data. This also applies to other Sensitive Data. Health Data are also increasingly becoming a target for cyber attacks. Humanitarian health-care providers should process data in accordance with the World Medical Association (WMA) International Code of Medical Ethics[16] 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;

16 WMA – The World Medical Association, *International Code of Medical Ethics*, 9 July 2018: www.wma.net/policies-post/wma-international-code-of-medical-ethics.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

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

Humanitarian Organizations engaged in protection or assistance activities may also process Health Data, for example, when this is necessary to locate persons unaccounted for (where Health Data may be required to identify and trace them) or to advocate for adequate treatment of individuals deprived of their liberty, or for the establishment of livelihood programmes addressing the needs of particularly vulnerable categories of beneficiaries (such as people suffering from malnutrition or particular diseases).[17]

2.6.2 ADMINISTRATIVE ACTIVITIES

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

2.7 DATA RETENTION

Each category of data should be retained for a defined period (e.g. three months, a year, etc.). When it is not possible to determine at the time of collection how long

17 See Subsection 2.5.2.1 – Further Processing.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

data should be kept, an initial retention period should be set. Following the initial retention period, an assessment should be made as to whether the data should be deleted, or whether the data are still necessary to fulfil the purpose for which they were initially collected (or for a further legitimate purpose). If so, the initial retention period should be renewed for a limited period of time.

When data have been deleted, all copies of the data should also be deleted. If the data have been shared with Third Parties, the Humanitarian Organization should take reasonable steps to ensure such Third Parties also delete the data. This consideration should be taken into account in initial reflections as to whether to share data with Third Parties and should be expressed in any data sharing agreement.[18]

2.8 DATA SECURITY AND PROCESSING SECURITY

2.8.1 INTRODUCTION

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

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

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;

18 See Section 2.12 – Data sharing and International Data Sharing, and Chapter 4: International Data Sharing.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

- methods of destruction of Personal Data;
- standard operating procedures for data management and retention;
- any other appropriate measures.

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

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

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

The Data Controller is responsible for:

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

- if feasible, keeping a historical log and potentially running audits of personnel having had access to a database, for as long as the data processed by such personnel are present in the database.

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

2.8.2 PHYSICAL SECURITY

Each Data Controller is responsible for:

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

2.8.3 IT SECURITY

The Data Controller should:

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

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

Remote access to servers and the use of home-based computers should comply with the standards set out in the Data Controller's IT Security Policy. Unless absolutely necessary for operational reasons, the use of Internet outlets and

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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.[19] Staff should check that they have logged off properly from computer systems and that open browsers have been closed.

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

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

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

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

2.8.4 DUTY OF DISCRETION AND STAFF CONDUCT

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

- all personnel and external consultants signing discretion and confidentiality agreements or clauses as part of their employment/consulting contract. This

19 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.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

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

2.8.5 CONTINGENCY PLANNING

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

2.8.6 DESTRUCTION METHODS

When it is established that retention of Personal Data is no longer necessary, all records and backups should be safely destroyed or rendered anonymous. The method of destruction shall depend, *inter alia*, on the following factors:
- the nature and sensitivity of the Personal Data;
- the format and storage medium;
- the volume of electronic and paper records.

The Controller should conduct a sensitivity assessment prior to destruction to ensure that appropriate methods of destruction are used to eliminate Personal Data. In this regard, the following three paragraphs are based on information taken from the *IOM Data Protection Manual*:[20]

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

20 International Organization for Migration (IOM), *IOM Data Protection Manual*, pp. 83–84.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

paper records should be converted into digital records, following accurate conversion of paper records to electronic format, all traces of paper records should be destroyed, unless retention of paper records is required by applicable national law, or unless a paper copy should be kept for archiving purposes. The destruction of large volumes of paper records may be outsourced to specialized companies. In these circumstances the Data Controller should ensure that, throughout the chain of custody, the confidentiality of Personal Data, the submission of disposal records and the certification of destruction form part of the contractual obligations of the Data Processors, and that the Data Processors comply with these obligations.

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

The Data Controller should ensure that all relevant contracts of service, memoranda of understanding (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 subcontractors. Disposal records indicating time and method of destruction, as well as the nature of the records destroyed, should be maintained and attached to project or evaluation reports.

2.8.7 OTHER MEASURES

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

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

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

2.9 THE PRINCIPLE OF ACCOUNTABILITY

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

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

- drafting Personal Data Processing policies (including Processing Security policies);
- keeping internal records of data Processing activities;
- creating an independent body to oversee the implementation of the applicable data protection rules, such as a Data Protection Office, and appointing a Data Protection Officer (DPO);
- implementing data protection training programmes for all staff;
- performing Data Protection Impact Assessments (DPIAs);[21]
- registering with the competent authorities (including data protection authorities), if legally required and not incompatible with the independence of an international organization or 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, this information should be provided before Personal Data are processed, although this principle may be limited when it is necessary to provide emergency aid to individuals.

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

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

2.10.1 DATA COLLECTED FROM THE DATA SUBJECT

Personal Data may be collected directly from the Data Subject under the following legal bases:[22]

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

Some of the information to be provided to Data Subjects in each of the above cases will vary depending on the particular circumstances. A priority in this respect is that the information provided must be sufficient to enable them to exercise their data protection rights effectively.[23]

2.10.2 INFORMATION NOTICES

In the specific cases where Consent may be used as the legal basis,[24] the individual must be put in a position to fully appreciate the risks and benefits of data Processing, otherwise Consent may not be considered valid.

When using Consent or when the Data Subjects are exercising their rights to object to the Processing or to access, rectify and erase the data, detailed information will need to be provided. It is important to note that the Data Subject may object to the Processing or withdraw their 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 their Personal Data and an explanation of the potential risks and benefits;
- the fact that the Data Controller may process their 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 they have given Consent, they 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 their rights;
- to which third countries or International Organization/s the Data Controller may need to transfer the data in order to achieve the purpose of the initial collection and Further Processing;

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

23 See Section 2.11 – Rights of Data Subjects.

24 See Section 3.2 – Consent.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

- the period for which the Personal Data will be kept or at least the criteria to determine it and any steps taken to ensure that records are accurate and kept up to date;
- with which other organizations, such as authorities in the country of data collection the Personal Data may be shared;
- in case decisions are taken on the basis of automated Processing, information about the logic involved;
- an indication of the security measures implemented by the Data Controller regarding the data Processing.

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

- the identity and contact details of the Data Controller;
- the specific purpose for Processing of their Personal Data;
- whom to contact in case of any questions concerning the Processing of their Personal Data;
- with whom the data will be shared, in particular if they 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.[25]

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.[26] Humanitarian Organizations should also refrain from collecting extensive data sets from affected populations until this information can be adequately provided, unless absolutely necessary for humanitarian purposes.

2.10.3 DATA NOT COLLECTED FROM THE DATA SUBJECT

Where the Personal Data have not been obtained from the Data Subject, the information set out under Section 2.10.2 – Information notices, 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

25 See Section 2.10 – Information, and Section 3.2 – Consent.

26 See Section 2.10 – Information.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

security constraints. This requirement will not apply where the Data Subject already has the information or where providing it is impossible or would involve a disproportionate effort, in which case the measures outlined above in Section 2.10 – Information should be considered.

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

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.[27]

2.11.2 ACCESS

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

27 See ICRC, "The ICRC Data Protection Commission", 22 January 2016: www.icrc.org/en/document/icrc-data-protection-independent-control-commission; "Commission for the Control of INTERPOL's Files (CCF)", accessed 17 October 2021: www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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

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

Access to documents does not apply when overriding interests require that access not be given. Thus, compliance by Humanitarian Organizations with a Data Subject's access request may be restricted as a result of the overriding public interests or interests of others. This is particularly the case where access cannot be provided without revealing the Personal Data of others, except where the document or information can be meaningfully redacted to blank out any reference to such other Data Subject/s without disproportionate effort, or where the Consent of such other Data Subject/s to the disclosure has been obtained, again without disproportionate effort.

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

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

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

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

2.11.3 CORRECTION

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

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

2.11.4 RIGHT TO ERASURE

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

- the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed and/or further processed;
- the Data Subject has withdrawn their Consent for Processing, and there is no other basis for the Processing of the data;[28]
- the Data Subject successfully objects to the Processing of Personal Data concerning them;[29]
- 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, for reasons of public interest in the area of public health, for compliance with an applicable legal obligation, for the establishment, exercise or defence of legal claims, or for legitimate historical or research purposes, subject to appropriate safeguards and taking into account the risks for and the interests of the Data Subject. This can include the interest in maintaining archives that represent the common heritage of humanity. In addition, Humanitarian Organization staff should require proof of identify that

28 See Section 3.2 – Consent.

29 See Section 3.4 – Important grounds of public interest, and Section 3.5 – Legitimate interest.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

satisfies them that the Data Subjects are who they say they are before carrying out any erasure.

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

2.11.5 RIGHT TO OBJECT

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

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

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

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

2.12 DATA SHARING AND INTERNATIONAL DATA SHARING

Humanitarian Emergencies routinely require Humanitarian Organizations to share Personal Data with Data Processors and Third Parties, including those based in other countries, or with International Organizations. Data protection laws restrict

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005

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.[30]

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

30 See Chapter 4: International Data Sharing.

Downloaded from https://www.cambridge.org/core. IP address: 13.58.130.38, on 04 Feb 2025 at 12:07:09, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009414630.005