CHAPTER 3

LEGAL BASES FOR PERSONAL DATA PROCESSING

3.1 INTRODUCTION

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

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

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

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

Processing by Humanitarian Organizations may often be based on vital interest or on important grounds of public interest,[1] for example in the performance of a mandate established under national or international law. This would require that the following conditions be met:

- in the case of vital interest, having sufficient elements to consider that in the absence of Processing the individual could be at risk of physical or moral harm. In the case of important grounds of public interest, being clear that the specific Processing operation is within a mandate established for the Humanitarian Organization under national, regional or international law, or that the Humanitarian Organization is otherwise performing a specific task or function that is in the public interest and is laid down by law.
- providing clear information to the individual as to the proposed Processing operation.
- ensuring the individual has a say and is in a position to exercise the right to object.[2] In any case, the opportunity to object to the Processing should be offered as soon and as clearly as possible, preferably at the moment of data collection. If the Data Subject provides adequate justification for their objection to the

1 See Section 3.3 – Vital interest, and Section 3.4 – Important grounds of public interest.

2 See Chapter 2: Basic principles of data protection.

Processing, and if the Processing is not necessary for any other legal basis (e.g. Section 3.3 – Vital interest, or Section 3.4 – Important grounds of public interest), then the Processing of the Data Subject's Personal Data should cease.

Relying on an appropriate legal basis does not discharge a Humanitarian Organization of its responsibility to assess the risk, for an individual, a given group or the Humanitarian Organization itself, of collecting, storing or using Personal Data. In cases involving particularly high risks, Humanitarian Organizations should consider whether it is not more appropriate to refrain from collecting and/or Processing the data in the first place. Such risks may be immediately evident from the Humanitarian Organization's experience or hidden in the complexity of the data flows inherent in a new technological solution. The performance of a Data Protection Impact Assessment (DPIA) therefore remains a key tool to ensure that all relevant risks are identified and mitigated.[3]

3.2 CONSENT

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

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

3 See Chapter 2: Basic principles of data protection.

alternative to the specific assistance being offered and the data Processing involved.

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

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

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

3.2.1 UNAMBIGUOUS

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

3.2.2 TIMING

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

3.2.3 VALIDITY

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

3.2.4 VULNERABILITY

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

Vulnerability varies depending on the circumstances. In this respect, the following factors should be considered:[4]

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

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

3.2.5 CHILDREN

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

4 International Organization for Migration (IOM), *IOM Data Protection Manual*, pp. 45–48.

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

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

3.2.6 INFORMED

Consent should be informed if it is to be accepted as the legal basis for Processing. This requires that the Data Subject receive explanations in simple, jargon-free language, which allows for full appreciation and understanding of the circumstances, risks and benefits of Processing.[5]

3.2.7 DOCUMENTED

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

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

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

3.2.8 WITHHOLDING/WITHDRAWING CONSENT

If Data Subjects expressly withhold Consent, they should be advised about the implications, including the effect this may have on assistance that might or might not be rendered by Humanitarian Organizations and/or Third Party organizations. If,

5 See Section 2.10 – Information.

however, assistance could not be provided in the absence of Consent, note that Consent could not be considered as a legal basis for the Processing.[6]

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

3.3 VITAL INTEREST

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

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

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

In these cases, however, the Humanitarian Organization should, if possible, ensure that the Data Subjects are aware of the Processing as soon as possible, that they have sufficient knowledge to understand and appreciate the specified purpose(s) for which Personal Data are collected and processed, and are in a position to object to the Processing if they so wish. This can be achieved preferably through direct

6 See Section 3.2 – Consent, fourth bullet point.

explanations at the moment of the collection and, for example, during distributions of assistance, using posters, group explanations or by making further information available on leaflets or on websites when affected people are registered or aid is distributed.[7]

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

3.4 IMPORTANT GROUNDS OF PUBLIC INTEREST

Important grounds of public interest are triggered when the activity in question is part of a humanitarian mandate established under national or international law or is otherwise an activity in the public interest laid down by law. This, for example would be the case for the International Committee of the Red Cross (ICRC), National Societies of the Red Cross/Red Crescent, the United Nations High Commissioner for Refugees (UNHCR), the United Nations Children's Fund (UNICEF), the United Nations World Food Programme (WFP), the International Organization for Migration (IOM), and other Humanitarian Organizations performing a specific task or function in the public interest, which is laid down by law, insofar as the Processing of Personal Data is necessary to accomplish those tasks.[8] In this case, the term 'necessary' is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,[9] to fulfil the relevant purpose).

7 See Section 2.5.1 – The principle of the fairness and lawfulness of Processing, and Section 2.10 – Information.

8 For example, the ICRC has a mandate under the four Geneva Conventions and Additional Protocol I to act in the event of international armed conflict. The ICRC has a right of humanitarian intervention in non-international armed conflict. See: ICRC, "The ICRC's Mandate and Mission", Page, International Committee of the Red Cross, Geneva, 6 August 2014: www.icrc.org/en/mandate-and-mission.

9 See example at Section 3.6 – Performance of a contract.

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

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

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

3.5 LEGITIMATE INTEREST

Humanitarian Organizations may also process Personal Data where this is in their legitimate interest, in particular, where it is necessary for the purpose of carrying out a specific humanitarian activity listed in their mission, and provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. In all of these situations, the term 'necessary' is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient,[10] to fulfil the relevant purpose).

Legitimate interest may include situations such as the following:

- The Processing is necessary for the effective performance of the Humanitarian Organization's mission, in cases where important grounds of public interest are not triggered.
- The Processing is necessary for the purposes of ensuring information systems and information security,[11] and the security of the related services offered by, or

10 See example at Section 3.6 – Performance of a contract.

11 Information security may include preservation of confidentiality, integrity and availability of information, as well as other properties such as authenticity, accountability, non-repudiation and

accessible via, these information systems, by public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services, and by providers of security technologies and services. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

- The Processing is necessary for the purposes of preventing, evidencing and stopping fraud or theft.
- The Processing of Personal Data is necessary for the purposes of anonymizing or pseudonymizing Personal Data.[12]
- The Processing is necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial, administrative or any out-of-court procedure.
- The Processing is necessary to make the work of the organization more effective and efficient.

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

3.6 PERFORMANCE OF A CONTRACT

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

reliability. See: International Organization for Standardization (ISO), "ISO/IEC 17799:2005 | Information Technology – Security Techniques – Code of Practice for Information Security Management", ISO Geneva, 2005–2006): www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/96/39612.html.

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

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

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

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

3.7 COMPLIANCE WITH A LEGAL OBLIGATION

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

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

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

- existence of the rule of law and separation of powers in the country requiring access to the data;

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

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

3.7.1 THE DISCLOSURE OF PERSONAL DATA TO AUTHORITIES

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

Humanitarian Organizations enjoying privileges and immunities as International Organizations should ensure that their specific status is respected and refuse to accede to such requests unless necessary in the best interest of the Data Subjects and Humanitarian Action. When a Humanitarian Organization enjoying privileges and immunities needs to transfer data to Humanitarian Organizations that do not enjoy such privileges and immunities, the risk that the recipient may not be in a position to resist such requests should be taken into account. This risk is specifically recognized in the International Conference of Privacy and Data Protection Commissioners' Resolution on Privacy and International Humanitarian Action of 2015:[13]

> *Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of*

13 International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy and International Humanitarian Action*.

migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to Humanitarian Action more generally.

As a specific measure to address this very concern, the 33rd International Conference of the Red Cross and Red Crescent in 2019, in its Resolution on Restoring Family Links while respecting privacy, including as it relates to Personal Data protection urged:[14]

States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement, [. . .], or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of RFL services.

14 International Conference of the Red Cross Red Crescent Movement, *Restoring Family Links While Respecting Privacy, Including as It Relates to Personal Data Protection*, Resolution, International Conference of the Red Cross Red Crescent Movement, December 2019, para. 11: https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.