CHAPTER 8

# BIOMETRICS

**Massimo Marelli***

* The author thanks Vincent Graf Narbel and Justinas Sukaitis for the input and feedback.

# 8.1 INTRODUCTION

The International Organization for Standardization defines biometric recognition and Biometrics as the "automated recognition of individuals based on their biological and behavioural characteristics".[1] Biometrics are therefore measurable and unique human signatures that may include fingerprints, iris scans or behavioural characteristics such as the way a person walks.

The data protection implications of the use of biometric data, with particular reference to the use of biometric data in passports, identity cards and travel documents, have been highlighted by the International Conference of Data Protection and Privacy Commissioners in its Resolution on Biometrics, adopted in Montreux, Switzerland, in 2005.[2]

Humanitarian Organizations around the world increasingly deploy biometric recognition as part of their identification systems because of the benefits it can bring in efficiently identifying individuals and preventing fraud and/or misuse of humanitarian aid. Indeed, paper-based identification mechanisms (identity cards, ration cards, wrist bands, etc.) that constitute the non-digital alternative have limitations, as they may easily be lost or counterfeited, require substantial resources to cross-check (thereby giving rise to potential duplication and inefficiency) and in most cases do not allow for automated Processing. In certain situations, it is suggested that these shortcomings may be overcome through the use of biometric identification systems (often as an additional means of verification). Biometric data are more difficult to counterfeit and, being digitally produced and stored, facilitate the efficient management of humanitarian aid in the field and can also be used for Data Analytics or other types of advanced data Processing operations. In addition, by focusing on the individual's unique features, Biometrics can confirm the identity of individuals who have no other means of adequately proving it, which is often the case with displaced people, and therefore put individual identity and dignity at the heart of Humanitarian Action.[3]

1 See International Organization for Standardization ISO/IEC 2382-37:2022 Information Technology - Vocabulary. Part 37: Biometrics. March 2022: https://www.iso.org/standard/73514.html.

2 International Conference of Data Protection and Privacy Commissioners, *Resolution on Use of Biometrics in Passports, Identity Cards and Travel Documents*, Resolution, 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 16 September 2005: https://edps.europa.eu/sites/default/files/publication/05-09-16_resolution_biometrics_en.pdf.

3 See for example: Hugo Slim, "Eye Scan Therefore I Am: The Individualization of Humanitarian Aid", European University Institute (blog), 15 March 2015: https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid; Paul Currion, "Eyes wide shut: The challenge of humanitarian biometrics", *The New Humanitarian* (formerly *IRIN News*), 26 August 2015, Online edition, sec. Solutions and Innovations | Opinions: www.thenewhumanitarian.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics.

However, these promises have not always been fulfilled in the actual deployment of Biometrics identification systems. Some projects to implement Biometrics have reportedly faced considerable problems with regard to the reliability of the relevant systems.[4] Inherent limitations, such as the fact that individuals' fingerprints are not always readable, provide further difficulties in implementation. Ethical issues also arise, for example, by virtue of the use of biometric data in national identification systems and the problematic legacies of such systems in certain countries.[5] Additionally, due to the interest in biometric data for national law enforcement and national security purposes, Humanitarian Organizations may find themselves under increasing pressure to share data with national and regional authorities for purposes which go beyond humanitarian work. At the same time, Third Parties may be interested in accessing biometric data also through unauthorized means, for example through hacking.

Humanitarian Organizations may use biometric technologies for Processing operations such as the collection and management of data on displaced persons who have to be registered for the purposes of humanitarian aid distribution, including aid delivered through cash and vouchers.[6]

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

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

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

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

4 Gus Hosein and Carly Nyst, *Aiding Surveillance*, Privacy International, 1 November 2013: http://privacyinternational.org/report/841/aiding-surveillance.

5 Ibid., 19.

6 See Chapter 9: Cash and Voucher Assistance.

- enhancing the resettlement of individuals into third countries;
- enabling bank account acquisition.

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

- reliability and accuracy of data (including the risk of false matches) and/or of systems – the quality of the biometric identification system ultimately depends upon the quality of the sensors used and the quality of the Biometrics provided;
- inherent technical difficulties (e.g. the unreadability of fingerprints in the case of certain people with depleted fingerprints);
- biometric information is unique and cannot be modified, consequently resulting in data leaks exposing affected persons to potential identity thefts through the synthetization of the biometric information;
- hardware and software modules of most current biometric systems are incompatible across different solution providers and thus may lock the Humanitarian Organization into a single vendor;
- as biometric data contains inherently more information about the individual than what is strictly necessary for authentication and even identification purposes (e.g. health-related information), Biometrics are excessive by nature;
- ethical issues (cultural sensitivities, affected people's perceptions and/or concerns about surveillance);
- function creep (same systems used for other purposes than the ones originally designated, including non-humanitarian purposes);
- possible pressure by various national or regional authorities (including donors) to acquire the biometric data sets collected by Humanitarian Organizations, with the risk of the data being used for purposes other than strictly humanitarian purposes (e.g. law enforcement, security, border control or monitoring migration flows).

It is very important, therefore, that Humanitarian Organizations carefully analyse and consider the possible need for the use of biometric data, and clearly and transparently set out how they intend to use them in a way that is compatible with Data Protection requirements, ideally through public policies on the use of biometric data.[7]

## 8.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The use of biometric technologies raises significant data protection issues. Biometric information is considered to be Personal Data and therefore covered by data

7 See for example: Massimo Marelli and Ben Hayes, "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy", Humanitarian Law & Policy Blog (blog), 18 October 2019: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy.

protection legislation. For example, the EU General Data Protection Regulation expressly regulates biometric data, defining them as "Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".[8] In many legal systems, biometric information is considered "Sensitive Data".[9] Consequently, special, detailed requirements apply to the Processing of this type of data, directly affecting the lawfulness of the Processing in the event that they are not met.

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

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

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

When undertaking DPIAs, Humanitarian Organizations should take into account the fact that different types of biometric data may have different levels of "sensitivity". Some categories of biometric data, while sensitive for the reasons set out above, may be more or less sensitive than others. Fingerprints, for example, may be depleted or erased, whether unintentionally (e.g. through heavy manual work) or intentionally, thus making this type of data less sensitive than others. Iris scans may potentially enable the extraction of very sensitive information beyond the identification of the individual. Furthermore, certain types of biometric data may only be collected and read with the direct participation of a Data Subject, such as palm vein recognition, thus making this type of data less sensitive than others. Other categories of biometric data, such as iris information, can be read from a distance, thus making it particularly sensitive.[10]

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

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

10 See for example: Patrick Tucker, "How Facial Recognition Might Stop the Next Brussels", Defense One, 22 March 2016: www.defenseone.com/technology/2016/03/how-facial-recognition-might-stop-next-brussels/126883.

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

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

## 8.2.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations may process Personal Data using one or more of the following legal bases:[11]

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

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

- the individuals' physical inability to provide it, such as in cases of unconscious patients (where, for example, biometric data may be required to unlock a patient medical file, combined with other legitimate authority to unlock);
- the shortage of time and staff to ensure adequate counselling during the first phases of an emergency, when the priority is to provide life-saving assistance;
- the individuals' vulnerability and/or legal inability to provide it;
- the highly technical and irreversible nature of the data potentially exposing individuals to risks that are difficult to understand or contemplate when Consent is given. This refers particularly to the possibility that science and technology may

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

develop in ways that pose new risks not foreseen at the time of Consent (e.g. genetic information becoming accessible from a scan of an individual's iris);
- no real choice is provided as to alternative ways of receiving assistance or protection (for example, if you are dependent on humanitarian aid for your survival or that of your family, or if you need to register to remain legally in the country in which you are located, there is very limited opportunity for you to refuse the collection of your biometric data).

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

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

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

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

A final consideration in this area relates to the intrinsic value of biometric data in establishing a clear and univocal identity to persons affected by Humanitarian

Emergencies and the role that this could have in restoring and/or strengthening their dignity and protecting their rights over their data. In this light, the vital interests of the individual as Data Subject may indeed be at stake.

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

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

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

### 8.2.2 FAIR AND LAWFUL PROCESSING

Under data protection law, Personal Data need to be processed lawfully and fairly.[12] Lawfulness of the Processing refers to the identification of an appropriate legal basis. The requirement for fairness is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations involved in biometric

12 See Section 2.5.1 – The principle of the fairness and lawfulness of Processing, and Section 8.2.2 – Fair and lawful Processing.

data Processing should keep in mind that these principles need to be applied during all stages of Processing.

### 8.2.3 PURPOSE LIMITATION AND FURTHER PROCESSING

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

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

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

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

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

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

As explained above,[13] purposes within the wider category of "humanitarian purposes" are likely to be compatible with Further Processing operations. This would, however, not be the case if new risks are involved, or if the risks for the individuals concerned outweigh the benefits of Further Processing. This assessment would depend on the circumstances of the case, and include an analysis of any risks that Processing may be against significant interests of the person to whom the information relates or his/her family, in particular, when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or reputation.

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

### 8.2.4 DATA MINIMIZATION

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

Biometric information collected for identification purposes needs to be proportionate to these purposes. This means that only the amount of biometric information necessary for the identification of individuals needs to be collected and processed; any information not relevant to the identification should be seen as "in excess" and not be collected and, if collected, should be deleted. In particular, once the raw biometric data have been processed and are ready to be stored for further use for authentication or identification purposes, any intermediary or original raw biometric data should be deleted.

Similarly, the range of biometric data sets collected should be limited to what is proportionate (e.g. collecting facial imagery or iris scans may not be considered as

13 See Section 8.2.3 – Purpose limitation and Further Processing.

proportionate if photos and fingerprints are already being used for identification purposes).

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

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

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

### 8.2.5 DATA RETENTION

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

### 8.2.6 DATA SECURITY

Given the sensitive nature of biometric information as well as its potential misuse if unauthorized access is granted to it or otherwise obtained,[14] it is imperative that adequate, proportionate security measures are implemented by the Humanitarian Organization determining the purposes and means of the Processing (i.e. by the Data Controller). For example, encryption or compartmentalization of information could constitute viable solutions to this end for Humanitarian Organizations.

14 Sarah Soliman, "Tracking Refugees with Biometrics: More Questions than Answers", War on the Rocks (blog), 9 March 2016: https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questions-than-answers.

### 8.2.7 "EXCESSIVENESS" BY NATURE

Part of the reason behind the sensitivity of biometric information is the fact that it involves excessive Processing by nature. Biometric systems and biometric information involve an intrinsic link between the data and the individual the data originate from. In the current state-of-the-art of biometric technology, Processing biometric data involves, by nature, Processing more information about the individual than is strictly necessary for authentication and, in the vast majority of cases, also for identification purposes. The data may reveal the individual's health, gender, ethnicity and other personal information.[15]

Though the risk may never be fully alleviated, Humanitarian Organizations should reach for a higher level of data security for Biometrics or even re-evaluate whether their needs and identified benefits for affected persons and communities outweigh this intrinsic risk.

## 8.3 RIGHTS OF DATA SUBJECTS

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

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

Adequate infrastructure should be put in place to facilitate the rights to access, objection, deletion and rectification when Biometrics are used. In this regard, it is

15 Daniel Hartung and Christoph Busch, "Why Vein Recognition Needs Privacy Protection", IEEE Press, 2009, pp. 1090–1095: https://doi.org/10.1109/IIH-MSP.2009.132; Justinas Sukaitis, "Building a Path towards Responsible Use of Biometrics", thesis, EPFL, Lausanne, 2021: https://infoscience.epfl.ch/record/285077; Stelvio Cimato et al., "Privacy in biometrics", in Nikolaos V. Boulgouris, Konstantinos N. Plataniotis and Evangelia Micheli-Tzanakou (eds.), *Biometrics: Fundamentals, Theory, and Systems*, Wiley–IEEE Press, Hoboken, NJ, 2010, 633–654.

advisable to define complaint procedures in internal data protection policies and implement them in Personal Data Processing practices.

## 8.4 DATA SHARING

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

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

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

## 8.5 INTERNATIONAL DATA SHARING

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

Data protection laws restrict International Data Sharing and Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Biometrics are used, as discussed above.[16] Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and their own internal policies before carrying it out. Performing a DPIA[17] prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing from a data protection perspective.

16 See Section 8.2.1 – Legal bases for Personal Data Processing.

17 See Section 8.7 – Data Protection Impact Assessments.

## 8.6 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

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

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

## 8.7 DATA PROTECTION IMPACT ASSESSMENTS

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

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