International Red Cross and Red Crescent Movement Family Links Network

Code of Conduct on Data Protection

Version 2.0

2024

Foreword

This Code of Conduct (CoC) was drafted by a working group made up of representatives from the Austrian Red Cross (Claire Schocher-Döring), Belgian Red Cross (Flanders) (Axel Vande Veegaete and Nadia Terweduwe), British Red Cross (Mark Baynham and Emily Knox), German Red Cross (Jutta Hermanns), Red Cross EU Office (Olivier Jenard), International Committee of the Red Cross (Romain Bircher, Massimo Marelli and Katja Gysin) and International Federation of Red Cross and Red Crescent Societies (Christopher Rassi). Several other representatives of these organizations also helped to draft this CoC, took part in discussions and meetings and made important contributions. The working group began discussions for this project in late 2013, and over the course of two years, members met several times in different European locations: Mechelen (April 2014), Brussels (July 2014), Vienna (September 2014), Sofia (November 2014), and London (January 2015). Members also had many conference calls and email exchanges. The working group adopted by consensus, incorporating feedback received from many National Societies.

The CoC was revised in 2024 by members of the CoC application group and some other representatives from the ICRC Data Protection Office and Protection of Family Links Unit (PFL Unit). The application group adopted the revised version of the CoC by consensus, incorporating feedback received from its members.

The CoC was deemed necessary because of (1) the many people and groups within the International Red Cross and Red Crescent Movement working for the Family Links Network, and the need to transfer data within the Movement and to other people and groups from outside the Movement, and (2) the changing regulatory environment in Europe and worldwide with regard to data protection laws and standards. The CoC sets out the minimum principles, commitments, and procedures that members of the Movement must comply with when processing data within the Family Links Network. The CoC seeks to comply with the most stringent data protection regulations, particularly the European Union legislation on this matter. When using the CoC, National Societies must also ensure that they comply with their own national legislation, which shall prevail if there are any conflicts with the CoC. The CoC is a reference document that is integrated into the Movement's main set of Restoring Family Links (RFL) guidance. Individual members of the Movement will need to adopt the CoC and incorporate it into their own standard procedures.

This CoC is a tool that all members of the Movement can use to protect the fundamental rights and freedoms of individuals involved in RFL activities, in particular their right to privacy and to the protection of their personal data. The CoC will hopefully instil confidence in both individuals and regulators with regard to the work of the Movement, and in members of the Movement who need to transfer data to one another for RFL cases.

Table of Contents

Definitions

International Red Cross and Red Crescent Movement

The Movement is a worldwide humanitarian movement whose mission is "to prevent and alleviate human suffering wherever it may be found, to protect life and health, and ensure respect for the human being, in particular in times of armed conflict and other emergencies, to work for the prevention of disease and for the promotion of health and social welfare, to encourage voluntary service and a constant readiness to give help by the members of the Movement, and a universal sense of solidarity towards all those in need of its protection and assistance".

The Movement is made up of the International Committee of the Red Cross (ICRC), the National Red Cross and Red Crescent Societies (National Societies) and the International Federation of Red Cross and Red Crescent Societies (IFRC).

Central Tracing Agency

The Central Tracing Agency (CTA) is a permanent service within the ICRC in accordance with the provisions of the four Geneva Conventions and their Additional Protocols and with the Statutes of the Movement. The CTA – in cooperation with other components of the Movement – carries out RFL activities to help people affected by armed conflict and other violence, natural disasters and other circumstances that require a humanitarian response. In line with the 1997 Seville Agreement and the supplementary measures adopted in 2005, and the 2008–2018 RFL Strategy for the Movement, the CTA has the lead role within the Movement in all RFL-related matters; it coordinates operations and acts as a technical adviser to National Societies.

Data controller

A data controller is any component of the Movement, which, alone or with others,[1] determines the purposes of and the methods for processing personal data.

Data processor

A data processor is a person, public authority, agency or other body that processes personal data on behalf of and upon instruction from a data controller (e.g. an IT service provider).

Data protection focal point for RFL

A data protection focal Point for RFL is a person or unit from each component of the Movement that is responsible for raising awareness of data protection and ensuring members of the Movement

[1] A brief explanation on controllership and joint controllership between the ICRC and National Societies is provided in annex 5.

comply with the CoC. The data protection focal point for RFL should have a strong background in RFL and understand data protection principles and obligations.

Data subject

A data subject is an individual who can be identified – directly or indirectly – by referring to personal data.[2]

To determine whether a person is identifiable, it is necessary to consider all the means that the controller or any individual are likely to use to identify a person, either directly or indirectly. To ascertain whether these means are likely to be used to identify an individual, it is necessary to consider all objective factors, such as the cost of identification and the amount of time it takes. It is important to consider the technology that is available when the data processing takes place, as well as any future technological developments. Personal data does not therefore include anonymous information, which does not relate to an identified or identifiable individual, or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. Given the capabilities of new technologies, it is difficult to ensure that anonymous information or information that is subject to an anonymization process is not used to identify the data subject. This CoC therefore does not cover the processing of such anonymous information, including for statistical and research purposes.

When using online services, individuals may be linked to online identifiers that are provided by their devices, applications, tools and protocols, such as Internet Protocol (IP) addresses or cookies. This may leave traces which, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. If information, such as numbers, location data, online identifiers (e.g. IP addresses or cookies), does not identify an individual or make an individual identifiable, it is considered anonymous and should not be considered as personal data.

Family members

The following people may be classed as family members:

- children born in and out of wedlock, adopted children and stepchildren
- life partners, whether married or not
- parents, including parents-in-law and adoptive parents
- brothers and sisters that are born to the same parents, different parents or adopted
- close relatives[3]
- any other person with whom there is a strong emotional bond, even if not connected by blood.

[2] For example, the person who opens a tracing request before a component of the Movement.

[3] In many socio-cultural contexts, a family includes all of the people who live under the same roof or who maintain close relationships with one another. Therefore, the concept of family has to be understood based on societal practice and recognition.

It is important to also consider the way in which family members are defined in the domestic laws of the countries involved.

Minor

Any individual below the age of eighteen years old, unless the laws related to the rights of the child state that the age of majority is attained earlier.

Other individuals

As well as the people that submit tracing requests and the missing people, RFL activities may concern other individuals, such as other family members, witnesses, neighbours, community leaders, other missing people, etc.

Personal data

Personal data are any information relating to an identified or identifiable individual. An identifiable individual is someone who can be identified, directly or indirectly, using an identifier such as a name, number, audiovisual materials, location data, online identifiers or using one or several factors that are specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal data do not include anonymous information, which is information that: (a) does not relate to an identified or identifiable individual or (b) has been rendered anonymous in such a way that the data subject is not or no longer identifiable.

Sensitive data

Personal data which are particularly sensitive in relation to a specific situation faced by the data subject and which might cause very serious harm (e.g. discrimination or repression) if mishandled or disclosed. Therefore, sensitive data need a higher level of attention and protection. To determine whether data are sensitive, a risk assessment needs to be carried out on the situation in which RFL and RFL-related activities are being conducted.

Biometric and genetic data, as well as data that concern a data subject’s health are always considered sensitive data, regardless of the situation. Other data, are determined on a case-by-case basis, depending on the situation. As a general and non-binding rule, data that reveal racial or ethnic origin, political opinions, religious/philosophical beliefs, or details of a data subject's sex life or sexual orientation may be sensitive.

For National Societies, the scope of sensitive data may vary depending on domestic legislation.

Personal data breach

A personal data breach is an accidental or unlawful breach of security that risks or leads to the destruction, loss, theft, alteration, or unauthorized disclosure of, or access to, personal data while they are being sent, stored or otherwise processed.

Process / processing / processed

Process / processing / processed refers to any operation or set of operations that is performed with personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, distribution or otherwise making available, or deletion. Transferring data, within or outside the Movement, constitutes a processing operation.

Recipient

A recipient is a person, public authority, agency or other body other that is not the data subject, the data controller or the data processor and that receives the personal data.

Referral

A referral is the process of connecting someone with a service that they need. It may involve sharing the missing person's personal data, as well as the data of the person who submitted the tracing request.

Restoring Family Links activities and Restoring Family Links-related activities

Restoring Family Links (RFL) is a generic term describing a range of activities that aim to prevent family members from getting separated from one another, to help people to re-establish and maintain contact with their loved ones and to find out what has happened to missing people.

These activities may be linked to other support services that affected people can be referred to, such as psychological, psychosocial, medical, legal and administrative services. Families may also be able to receive material assistance, as well as access to resettlement and reintegration programmes and social welfare services (see annex 1 for details).

RFL services

National Societies and ICRC delegations around the world have members of staff within their organizations who are responsible for developing and implementing RFL activities and RFL-related activities.

The Family Links Network

When families are separated and people are missing because of armed conflict and other violence, natural disasters, migration or other humanitarian crises, we must do everything in our power to find out what has happened them, restore contact between them and their relatives and, if appropriate, reunite them.

The National Societies' RFL services and the ICRC form a single worldwide network called the **Family Links Network** (FLN). The CTA acts as technical adviser to and coordinator of this network, which mobilizes staff and volunteers on a global scale and ensures that RFL work is conducted according to the same principles and methodology all around the world.

More information on the FLN is available on the RFL website: http://familylinks.icrc.org.

Vulnerable person

In the context of this CoC, a vulnerable person is any individual who (i) has particularly suffered from the emotional and psychological impact of being separated from their loved ones and from the conditions they have had to face or (ii) cannot fully appreciate the risks and/or opportunities involved in data processing due to its complexity.

1. Introduction

1.1 Purpose of this CoC

This CoC sets out the minimum principles, commitments, and procedures that RFL staff from the ICRC, National Societies, and the IFRC must comply with when processing data within the framework of RFL activities, in order to: (1) comply with applicable data protection standards and legislation, (2) enable personal data to be passed seamlessly from one person to another for the purposes of RFL activities and (3) protect the fundamental rights and freedoms of the people who submit the tracing requests, the missing people and other individuals involved in RFL activities, such as witnesses or other family members, in accordance with International Humanitarian Law (IHL), International Human Rights Law and other international standards, in particular the right to privacy and to the protection of personal data.

1.2 Scope of this CoC

1.2.1 Restoring Family Links

This CoC applies to the processing of personal data in the context of RFL activities and RFL-related activities (see annex 1).

1.2.2 Personal data

This CoC applies to the processing of the personal data of people who submit tracing requests, missing people and other individuals related to RFL activities (including deceased people) by the data controllers.

1.3 The Family Links Network

The 1949 Geneva Conventions, their 1977 Additional Protocols, the Statutes of the Movement, resolutions adopted by the Council of Delegates and resolutions passed during the International Conference of the Red Cross and Red Crescent, provide the data controllers with a mandate to engage in RFL activities.

The National Societies execute this mandate alongside their respective public authorities in the humanitarian field, and they have a unique role in RFL worldwide. They work with the public authorities to organize different services to help victims of armed conflict, natural disasters and other emergencies.

1.4 Principles and Guidelines of the Movement

1.4.1 Fundamental Principles

The data controllers carry out their activities in accordance with the Fundamental Principles guiding the Movement: humanity, impartiality, neutrality, independence, voluntary Service, unity, and universality. All processing of personal data carried out by data controllers' RFL services is to be compatible with these principles.

1.4.2. Do no harm

The data controllers' RFL services do their utmost to avoid harming people when processing their personal data.

1.4.3 Confidentiality or Rules of disclosure

When data subjects share information with data controllers in confidence, data controllers must respect and ensure that this information remains confidential. Data controllers comply with all applicable national, regional or international legal obligations and are subject to the restrictions outlined in this current section (1.4). In order to determine which of these obligations are applicable, reference will be made to: (1) any privileges and immunities or waivers of obligations enjoyed by the data controllers in the country or region in question and (2) any legal protections as set out by international law, including IHL, and the mandate under the Statutes of the Movement.

1.4.4 Existing operational guidelines

The processing of personal data is carried out according to RFL guidelines that are provided by the Family Links Network, such as *Restoring Family links: A guide for National Red Cross and Red Crescent* Societies[4], *Assessing Restoring Family Links Needs – Handbook for National Societies and the ICRC*, *Restoring Family Links in Disasters – Field Manual* and *Professional Standards for Protection Work.*[5]

2. Basic principles for data processing and data controller commitments

2.1 Specified purpose

When collecting data, data controllers will determine and set out the specific, explicit and legitimate reason(s) as to why the data are being processed.

Data are primarily processed to restore contact between relatives that have been separated as a result of armed conflict and other violence, natural disasters, migration or other situations requiring a humanitarian response.

In certain cases, further processing may be necessary for RFL-related activities, such as archiving, scientific or historical research or statistical purposes. The reason(s) for data processing may therefore differ from those that are initially specified at the time of collection. However, regardless of the purpose, all data processing must comply with all relevant data protection laws (see annex 1 for details).[6]

[4] https://www.icrc.org/en/publication/0784-restoring-family-links-guide-national-red-cross-and-red-crescent-societies

[5] Relevant guidance documents can be found on the Restoring Family Links extranet.

[6] To determine whether or not the purpose(s) for the further processing is compatible with the initial purpose(s), the data controller should consider the connection between the initial purpose(s) and the purpose(s) of the further processing, the context in which personal data were collected, including the reasonable expectations of the data subject, and the potential effects on the data subject.

2.2 Lawful and fair processing

All processing of personal data by the data controller must be carried out under one or more of the following legal bases:

- public interest
- vital interest of the data subject or of other individuals
- consent of the data subject
- legitimate interest of the data controllers
- compliance with a legal obligation.

When launching a data processing operation, the data controller must identify a legal basis that would render the data processing lawful. If an appropriate legal basis is identified, a data subject is still able to exercise their rights.[7]

2.2.1 Public interest

This legal basis is triggered when data processing is part of an FLN member's humanitarian mandate, as established under international or national law, or is otherwise an activity that is deemed to be in the public interest according to the applicable law. It is fundamental for RFL activities; however, it is not always recognized in domestic legislation, and so National Societies should first check whether their domestic law would allow them to rely on it as a legal basis for data processing.

The RFL and RFL-related activities that are carried out by data controllers are in the public interest because they are exclusively humanitarian in nature, as outlined in section 1.3 above. (For examples, see annex 2).

2.2.2 Vital interest

When data processing is necessary to protect the life, integrity, health, dignity or security of beneficiaries, the processing of personal data is considered to be in these people's vital interest. For example, if a data subject was so vulnerable that providing RFL services would be a life-saving matter.

2.2.3 Consent of the data subject

From a protection point of view, consent is essential for ensuring that RFL services are transparent and that beneficiaries are directly involved in them. In the context of data protection in this CoC, consent is one of the legal bases required in order for data processing to take place. Consent is to be given unambiguously using any appropriate method that enables a freely given, specific, and informed indication of the data subject's wishes, whether that's a written, oral, or other type of statement or a clear affirmative action by the data subject, giving their consent for their personal data to be processed.

Consent provides a legal basis for all processing activities that are carried out to fulfil the original purpose or for other, compatible purposes. If data controllers wish to start other processing

[7] See chapter 3 of this CoC.

operations for further and incompatible purposes, they need to find a new legal basis or seek additional consent from the data subject.

Consent can be given with limitations and the data subject has the right to withdraw their consent at any time. Details of the consent given, the level of confidentiality required, and any applicable limitations are recorded and kept with the personal data throughout the processing operation.

2.2.4 Legitimate interest

Personal data are also processed in circumstances where it is in the legitimate interest of the data controller to do so, and provided that the interests or the fundamental rights and freedoms of the data subject do not override that legitimate interest (for examples, see annex 3).

2.2.5 Compliance with a legal obligation

Data controllers will also comply with all applicable legal obligations when processing personal data, for example, they comply with national and regional legislation and court orders, and they are subject to the Fundamental Principles of the Movement. Legal obligations may differ between countries and situations.

2.3 Processing Commitments

2.3.1 Responsibility / Accountability

Data controllers ensure that data processors – that is any person or entity who has access to personal data and acts under the instructions of the data controllers – process personal data in a way that complies with this CoC. Data controllers also ensure that the responsibilities of each entity involved in processing personal data are clearly allocated and are specified in appropriate contractual clauses or other legally binding acts.

Sometimes a processor may need to hire another processor (a sub-processor) to carry out specific processing activities on behalf of the data controller. If this is the case, the processor must first inform the data controller, which then decides whether or not to authorize the sub-processor. The sub-processor will be subject to the same contractual responsibilities and obligations as the processor.

See section 4 below for further information on transferring data to third parties, who may not process the data exclusively in accordance with the data controller's instructions.

2.3.2 Processing adequate, relevant and updated data

Adequate data: personal data processed by the data controller's RFL services will be kept under review to ensure that they are adequate, relevant and not excessive for the purposes for which they are collected and processed. If archived, personal data will not be subject to review, as they serve scientific, historical, and statistical purposes.

Data accuracy: personal data will be sufficiently accurate, complete and up to date for the purpose for which they are collected and processed.

2.3.3 Data protection by design and by default

When designing data management systems and setting up procedures for the collection of personal data, appropriate technical and organizational measures will be taken to ensure they meet the requirements set out in this CoC.

2.3.4 Data Protection Impact Assessment (DPIA)

In situations where data processing is likely to involve significant risks to the rights and freedoms of data subjects, such as transfers, publication and disclosure, the data controller will carry out a DPIA prior to processing. If possible, the data controller will consult the data protection focal point for RFL and other stakeholders involved in developing the data processing project[8], in order to determine and evaluate:

- the benefits of processing the data
- the origin, nature, likelihood and severity of these risks
- the appropriate measures to be taken in order to demonstrate that the risks are minimized and that personal data are processed in accordance with this CoC and any applicable laws.

The level of risk, and hence the need to conduct a DPIA, is determined by a series of factors including, but not limited to, the scale, scope and context of the processing activities, the methods used to process data, such as use of automated technologies, the nature and sensitivity of the personal data processed, and the vulnerability of the data subject.

A DPIA should minimize the risk of harm to the data subject and/or the possible encroachment on their rights and freedoms. The data controller will document the outcome of the DPIA and the reasons why that outcome has been reached. The data controller will also ensure that any steps taken as a result of the DPIA are properly implemented and that they have the desired effect.

In the event of emergencies, it may not be possible to conduct a DPIA before data processing begins. It will therefore be done after the processing, as soon as reasonably possible.

2.3.5 Data retention

When personal data are no longer needed for the purposes for which they were collected, for further processing, or for processing on other legitimate/lawful grounds, they will be archived or deleted in accordance with the data controller's data retention policy (see also section 3.3).

The data controller shall incorporate the management of personal data into their internal procedure, including the storage of data for archiving purposes.

[8] All roles involved in developing the project should be included, e.g., IT, legal, protection, archives and information management, etc.

2.3.6 Data security

Depending on availability, reasonable technical, physical and organizational security measures will always be taken at every stage of data processing operations to prevent personal data from being accidentally or unlawfully destroyed, lost, stolen, altered, accessed or disclosed. Personal data can be accessed only by data controller staff, who require this access to deliver a specific service or task, with safeguards and access restrictions in place (see annex 3 for details).

2.3.7 Personal data breaches

Whenever the data controller becomes aware of a personal data breach, they shall notify the data subject without undue delay if the breach is likely to put the data subject's rights and freedoms at significant risk.

If the data controller is subject to specific domestic legal requirements concerning data breaches, they shall evaluate whether or not they have an obligation to notify State authorities if a breach occurs.

If a personal data breach affects cases that are shared with other members of the FLN, the CTA must inform the relevant National Societies and the ICRC without undue delay to ensure that the FLN can coordinate an appropriate response, including notifying the affected data subjects.

The purpose of notifying a data subject of a personal data breach is to minimize the risks faced by the data subject. The data controller will carry out an assessment prior to the processing to establish the level of risk faced by the data subject and to determine whether the data subject needs to be notified if a breach occurs.

If one or more of the following situations applies, the data controller may decide that it is not necessary to inform the data subject of a personal data breach:

- The data controller has implemented appropriate organizational, technological or physical security measures, and those measures were applied to the data affected by the personal data breach.
- The data controller has taken subsequent measures which ensure that the data subject's rights and freedoms are no longer likely to be put at particularly serious risk.
- Informing the data subject would involve disproportionate effort, in particular owing to the logistical or security conditions in place, or the number of cases involved. In this situation, the data controller will instead consider whether it would be appropriate to issue a public communication or use a similar measure whereby the data subjects are informed in an equally effective manner.
- Informing the data subject would contradict substantial public interest conditions and would undermine the viability of the data controller's operations.
- Given the security conditions in place, approaching the data subject could endanger or cause severe distress to the data subject themselves.

If the data controller deems it necessary to notify the data subject, they shall identify and use the best channel of communication to ensure the data subject receives the information in an appropriate way, given the situation.

3. Rights of Data Subjects

3.1 Information and Access

Information: The data controller is obliged to provide the data subject with information in a transparent manner. This is a core principle that will apply regardless of the legal basis for processing the data. It states that, when collecting personal data, or as soon as possible thereafter, the data controller will provide the data subject – provided logistical and security constraints allow – with information on the processing of their personal data, either orally or in writing.

The data subject should receive explanations in simple language, either orally or through other appropriate means, such as a written information notice. As a minimum, the following information must be provided:

- the identity and contact details of the data controller(s)
- the specific purpose for processing their personal data
- 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
- the data subject's right to access, correct and delete their personal data, as well as to withdraw consent, object to processing and insist on certain limitations
- an indication of how long records are kept for (data retention period) and the criteria used to determine that period
- the fact that their personal data may be shared with third parties, such as other organizations (including other components of the Movement), the State authorities in the country of data collection or another country or may be publicly disclosed and that their approval is required if their personal data are to be used as explained.

The applicable domestic legislation must be respected and could require the National Societies to include additional information for the data subject.

Access: At any time, data subjects have the right to request confirmation as to whether or not their personal data are being processed. If their data are indeed being processed, they are entitled to obtain access to them and information about why the data are being processed, who has access to them and what safeguards have been put in place.

Upon request and where technically feasible, a copy of the document(s) containing their personal data is provided.

Before granting access, the data controller should assess the viability of the access request, as well as the identity of the person submitting the request. Access to data needs to be restricted for the following reasons:

- overriding public interest including, but not limited to, confidentiality
- data protection interests and rights and freedoms of others
- the documents in question cannot be meaningfully edited because of security reasons and emergency situations
- the request is manifestly unfounded or excessive.

The data controller will maintain a record of access requests, and the outcome of such requests, including the categories of personal data accessed and/or the denial of access to information.

3.2 Disclosure to family members and guardians

A family member or the legal guardian of a child or other data subject in a vulnerable situation may request the disclosure of their relative or ward's personal data. This is usually presumed to be in the best interest of the data subject and therefore granted, unless there is sufficient reason to believe otherwise. The data subject should be consulted, where possible, in order to determine whether they object to such disclosure.

3.3 Rectification and Deletion

Rectification: When a request to rectify personal data is made, the data controller has to first identify the person that submitted the request and determine the feasibility of the request. The data controller will then respond to requests, in particular if the data are inaccurate or incomplete. This will apply to archived data too. The data controller will inform any recipients of the data of the rectifications that have been carried out, unless the rectification is not significant, or unless informing them involves a disproportionate effort.

Deletion: A data subject has the right to have their personal data deleted from the data controller's active databases in any of the following cases:

- They are no longer needed for the purposes for which their personal data was collected or are not needed for further processing.
- The data subject has withdrawn their consent for processing and there is no other legal basis for the processing of their personal data.
- The data subject objects to their personal data being processed.
- The processing of a data subject's personal data otherwise does not comply with this CoC or with the domestic legislation applicable to the National Societies.

If the personal data have been published, the data controller shall take reasonable steps, including technical measures, to remove the data from the public domain, including any links or copies of such data.

However, a data subject's personal data may be stored if this is necessary or justified, as in the following circumstances:

- for historical, statistical and scientific purposes, such as for documenting action taken by a data controller while carrying out its mandate under the Geneva Conventions of 1949 and their Additional Protocols, and/or the Statutes of the Movement
- for reasons of public interest
- for long-term humanitarian purposes
- to establish, exercise or defend legal claims

- with a view to the publication by any person of any journalistic, literary, or artistic material, for exercising the right of freedom of expression and information.

Moreover, a data subject's personal data may be stored if required by law. All requests shall be documented by the data controller, and the data subject will be notified of any decisions that are made regarding their request.

When data controllers receive a request to have personal data deleted, they will explain the impact that deleting the data will have on the provision of RFL services to the data subject. The data controller reserves the right to reject a request for rectification or deletion from the data subject if it considers that the data subject may have made the request under undue pressure and/or if deletion would be detrimental to the data subject's vital interests.

The data controller will inform anyone they shared the personal data with that the data have been deleted and will request that these recipients delete any links or copies of such data, unless the deleted data are not significant or unless communication involves a disproportionate effort. If recipients are FLN members, they shall inform the data controller of the decision taken about deleting the data without undue delay.

3.4 Objection to the processing

At any time, a data subject has the right to object to having their personal data processed if the legal basis for processing is that it is in the public interest or in the data controller's legitimate interests. The relevant personal data will no longer be processed unless the data controller demonstrates legitimate grounds for overriding the objection and continuing to process the data.

The data controller will inform any recipients of the data of the objection.

3.5 Right to withdraw consent

When the legal basis for data processing is consent, a data subject has the right to withdraw their consent at any time. If this occurs, the data controller takes all reasonable steps to stop processing and delete the data. If the data were transferred to a third party, the data controller should inform them that the data subject has withdrawn their consent so that the third party can also delete the data accordingly.

3.6 Remedies

A data subject addresses their request to the data controller, which then provides an answer within a reasonable timeframe or, in any event, within any timeframe imposed by law.

The staff that receive a request from a data subject will check the identity of the data subject using any reasonable method and will also do one of the following:

- agree to the request and notify the data subject that submitted the request of how the request was or will be fulfilled
- inform the data subject that submitted the request why the request will or cannot be fulfilled and inform them that they may file a complaint against the data controller.

4. Special provision on data transfers

4.1 General principles

4.1.1 Background

RFL and RFL-related activities often involve transferring personal data across borders from one data controller to another.

Data controllers may also need to transfer personal data to entities such as non-governmental organizations (NGOs), international organizations, public authorities, and other third parties whose services are needed to carry out RFL and RFL-related activities.

These transfers are carried out in accordance with FLN activities, as outlined in section 1.3, and as such the data subject must be duly informed when a transfer takes place and there must be a legal basis for a transfer to be carried out, i.e. it is in the public interest, it protects the vital interests of the data subject or other individuals, or the data subject has given their consent. Transfers must also comply with the principles and guidelines of the Movement, as set out in section 1.4.

4.1.2 General principles applicable to data transfers

Transferring data, whether it is within or outside the Movement, constitutes a processing operation. As such, transfers are subject to the basic principles set out in chapter two and to the rights of data subjects set out in chapter three. However, transfers are a particularly sensitive processing operation, and so certain requirements are particularly important, such as DPIAs, information for the data subject and data security.

As mentioned in section 3.1, the data subject should be informed of the reasonably foreseeable transfer of their personal data to third parties prior to/at the time of data collection.

To transfer personal data to people or organizations, appropriate and proportionate safeguards, including those mentioned in sections 4.1.4 and 4.1.6, and technical and organizational security measures, including those listed in annex 3, must be put in place. The sensitivity of the data, how urgently the situation requires humanitarian action, and logistical and security constraints, as detailed in this CoC, should be taken into account. In any case, the do-no-harm principle must always be taken into account.

4.1.3 Data Protection Impact Assessment for data transfers

The requirement to carry out a DPIA is particularly important in the context of data transfers. Therefore, if transferring data is likely to involve significant risks to the rights and freedoms of data subjects, the data controller will carry out a DPIA (see annex 6 for guidance) prior to the transfer, as set out in section 2.3.4 above. The DPIA will take into account the following elements:

- the national data protection laws and regulations that apply to the data transfer
- the security situation, respect for human rights and IHL, and the safety of data subjects in a particular country
- whether anonymous/aggregate data would suffice, or whether it is necessary to transfer data that may enable the data controller to identify the data subject

- the means and conditions of the data transfer
  the possibility of implementing a contractual obligation to prevent third parties from subsequently transferring the data to other third parties (onward transfers)
- the data subject's level of vulnerability as additional safeguards to protect confidentiality and anonymity may need to be put in place.

In any case, the data controller should not proceed with a data transfer when it is likely to harm the data subject in some way.

4.1.4 Conditions

Data transfers are subject to the following, cumulative conditions:

- A DPIA shall be carried out beforehand if the transfer is likely to involve significant risks to the data subject.
- The recipient of the transfer must process the data in accordance with the specified reasons for data processing and any compatible purposes.
- The recipient shall receive only the amount and type of personal data that is necessary to fulfil the specified purposes or further processing purposes.
- The transfer must be compatible with the data subject's reasonable expectations.

The data controller will assess the risks involved in transferring certain personal data to certain organizations to ensure the do-no-harm principle is upheld.

4.1.5 Documenting data transfers

The data controller will keep track of transfers, transfer methods and recipients of personal data.

4.1.6 Data sharing agreements

As set out in section 4.1.2, personal data may be transferred if the data controller is satisfied that appropriate safeguards are in place to ensure the personal data will be protected by the recipient. These appropriate safeguards may be established through data sharing agreements between data controllers and third parties whenever regular transfers of data are envisaged. These agreements will state very clearly that personal data will be transferred only for the purposes described within the agreements and any further, compatible purposes. They will also state the technical and organizational measures that will be implemented to ensure the data are protected during the processing.

Transfers of personal data within the Movement do not require a data sharing agreement because components of the Movement shall abide by the provisions of this CoC.

The data protection focal point for RFL must be involved to support the drafting of such agreements or equivalent legal acts.

Even when the parties involved sign agreements, the operational context may evolve and it may no longer be considered safe to transfer certain categories of data to certain recipients. This shall entail a prior assessment based on the do-no-harm principle.

4.2 Methods of transmission

In the event of a data transfer, appropriate measures will be used to safeguard the transmission of personal data to third parties. The level of security adopted and the method of transmission will correspond to the nature and sensitivity of the personal data, and to the risks highlighted by the DPIA.

5. Special provisions on data publication

5.1 General principles

The publication of personal data by the data controller constitutes a processing operation. As such, it is subject to the general principles set out in chapter two and the rights of data subjects set out in chapter three. However, publication is a particularly sensitive processing operation. Once data are published, the data controller and the data subject lose, to a large extent, control over the way in which the data are being processed. Therefore, the additional principles set out in this chapter will also be followed.

Depending on the results of DPIAs and on applicable legal obligations, the data controller's RFL services may publish personal data in order to restore contact between relatives separated by armed conflict and other violence, natural disasters and migration. These data may include names, photographs, statuses (such as alive and well, wounded, deceased, missing, displaced) and may be published online, in the media, on posters, in leaflets or via other suitable tools.

In accordance with section 2.2.1, public interest is the preferred legal basis for the publication of personal data.

5.2 Data Protection Impact Assessment for data publication

The requirement to carry out a DPIA, as set out in section 2.3.4 and annex six, is particularly important in the context of data publication.

In addition to the elements set out in section 2.3.4, in the context of publication, the DPIA for publications will take the following elements into account:

- the national data protection laws and regulations that apply to the publication of the data
- the security situation, respect for human rights and IHL, and the safety of data subjects in a particular country
- whether anonymous/aggregate data would suffice, or whether it is necessary to publish data that may enable the data controller to identify the data subject, and if the latter, whether other means to protect the identity of data subjects will serve or hinder the specified purpose of publishing the data (these other means may include not associating a photograph with names, distinguishing features, precise locations, etc.)
- the method and conditions of publication
- the possibility of implementing a requirement to prevent third parties from using the published data

- the possibility of specifying the period during which certain data may remain published on a particular media platform and the method of destruction that should be used after the specified purpose of publication has been fulfilled
- how useful and appropriate the publications are through regular evaluations by the data controller
- the importance of protecting vulnerable people from public curiosity in the context of public communication.

If the data subject is a vulnerable individual, additional considerations will, where appropriate, be taken into account, including additional safeguards to protect confidentiality and anonymity. The best way to protect data subjects is to uphold the do-no-harm principle.

5.3 Data to be published for RFL

If data are to be published, they need to be follow the guidelines for each given context, and more specific guidance may be available in relation to specific categories of data subjects. Depending on the results of the DPIA, specific mitigation measures may include:

- adopting a do-no-harm approach
- limiting publication to only the data that are absolutely necessary to enable the reader/listener to identify the people whose names/photographs are published and to put them back in contact with their relatives
- prohibiting photographs of vulnerable people from being published alongside other personal data (e.g. names), and never publishing the address of a minor.

5.4 Data to be published for public archives

Personal data that has been archived can become public in line with applicable legislation.

5.5 Data to be published for public communication

Personal data may be published in order to promote RFL activities and/or to raise awareness of situations of concern, provided the publication complies with applicable legislation. To publish data for this specific purpose, the data controller must first obtain consent from the person submitting the tracing request. Public communication is also linked to freedom of information and expression and to public accountability. However, as with any publication, the principles set out in this CoC will be followed and a DPIA will be carried out.

6. Application of the CoC

A CoC application group will help to implement the CoC on a global level by promoting continuous learning and development.

As well as being subject to national legislation, all data controllers must apply the present CoC as follows:

- ensure the CoC is reflected in RFL policies, guidelines and programmes
- ensure the CoC becomes an integral part of RFL staff management and is used as a training tool for each data controller
- appoint a data protection focal point for RFL in any entities that are part of the FLN and share contact details in order to develop a data protection network
- participate in regular surveys on the implementation of this CoC
- cooperate with the CoC application group
- conduct self-assessments, engage in dialogues, carry out peer reviews and other forms of review on a voluntary basis to ensure continuous improvement and learning across the Movement.

The CoC application group will review and update this CoC as and when required.

7. References

7.1 Legal instruments/guidance

UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990.

International Covenant on Civil and Political Rights, Art. 17.

Rallo Lombarte, A., *International Standard on the protection of personal data and privacy*: *The Madrid Resolution: International Conference of Data Protection and Privacy Commissioners*, *5 November 2009*, Spanish data protection agency, Madrid, 2009.

Council of Europe, Convention for the protection of individuals with regard to the processing of personal data, 108, 28 January 1981, BRON.

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, *OJ* L 281 23 November 1995, p. 31–50.

European Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8.

Treaty on the Functioning of the European Union, Art.16.

The Charter of Fundamental Rights of the European Union, Arts 7 and 8

Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD Publishing, Paris, 2002

OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD Publishing, Paris, 2000

Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, APEC Secretariat, Singapore, 2005.

Statutes of the International Red Cross and Red Crescent Movement, as amended in 2006.

ICRC, *Resolution 4 of the 2007 Council of Delegates on the Restoring Family Links Strategy for the International Red Cross and Red Crescent Movement*, ICRC, Geneva, 2007.

37th International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy and International Humanitarian Action*, Amsterdam, 2015.

33rd International Conference of the Red Cross and Red Crescent, *Resolution 4 – Restoring Family Links while respecting privacy, including as it relates to personal data protection,* 33IC/19/R4, ICRC, Geneva, 2019.

Council of Delegates of the International Red Cross and Red Crescent Movement, *Resolution 12 on Safeguarding humanitarian data*, CD/22/R12, ICRC, Geneva, 2022.

7.2 Doctrine

ICRC, *Restoring Family Links in Disasters: A Field Manual*, ICRC, Geneva, 2009, 211 pp.

ICRC, *Assessing Restoring Family Links Needs: A Handbook for National Societies and the ICRC*, ICRC, Geneva, 2010, 103 pp.

ICRC, *Guidelines on Providing Restoring Family Links Services to Persons Separated as a Result of Migration: An Internal Document for the International Red Cross and Red Crescent Movement*, ICRC, Geneva, 2010, 59 pp.

ICRC, *Restoring Family Links Strategy: Including Legal References*, ICRC, Geneva, 2009, 64 pp.

Morgan, O., Tidball-binz, M., Van alphen, D. (*eds), Management of Dead Bodies After Disasters: A Field Manual for First Responders*, Pan American Health Organization, Washington D.C., 2009, 53 pp.

Annexes

Annex 1: RFL activities and RFL-related activities

RFL activities – Depending on the situation and the context, there are different types of activities:

- organizing the exchange of family news
- tracing individuals
- registering and monitoring individuals (children or adults) to prevent their disappearance and to keep their families informed of their whereabouts
- reuniting families and repatriating people
- collecting, managing and forwarding information about the deceased
- transmitting official documents, such as birth certificates, identity papers or other certificates issued by the authorities
- issuing attestations of detention and other documents that provide information about situations concerning registered individuals
- issuing ICRC travel documents
- monitoring people who have been reunited with their relatives to ensure they are adjusting well
- promoting and supporting systems to find out what has happened to missing people.

RFL-related activities – These are other humanitarian services that are related to RFL activities and carried out by RFL staff. They include:

- providing material, legal, psychological and psychosocial support to the families of missing people and other individuals affected by armed conflict and other violence, natural disasters, migration and other humanitarian crises
- supporting the relevant authorities in managing human remains and conducting forensic identifications
- helping families of missing people, unaccompanied minors and vulnerable people (either directly by the FLN or through referrals to external parties)
- providing resettlement services or (referrals to) reintegration support services to vulnerable groups of people
- archiving for a range of different needs, such as individual/family memories, collective memories of humanity, individual administrative needs, accountability of the parties involved, and historical, statistical, and medical research
- managing public relations to promote RFL and RFL-related activities.

Annex 2: Legal bases

a. Public interest

Public interest is used as a lawful basis when:

- dealing with large-scale crises that require immediate action, and the data subject can understand the information being provided and react to their personal data being shared and/or published.
- the processing operations are very complex, involving different external processors and complex technologies, making it difficult for data subjects to fully appreciate the risks and benefits of the processing steps involved. If the vital interests of the data subject or of another individual cannot be established (due to a lack of urgency), the data controller's mandate may be used as grounds for the processing, provided a satisfactory DPIA is carried out.
- distributing assistance, and it is not possible to obtain the consent of all the beneficiaries involved, and the life and integrity of the data subject or of other people are not likely to be at stake (in which case, vital interest may be the most appropriate basis for processing).
- processing the personal data of a data subject in detention. This may happen, for example, when an individual is deprived of their liberty because of armed conflict or other violence, and the ICRC (or National Society) has not yet been able to visit the data subject to obtain their consent, and the prevailing detention conditions in the case in question could prevent vital interest from being used as a lawful basis.
- processing the personal data of unaccompanied minors, who do not have the legal capacity to provide valid consent, and when the conditions that would trigger the use of vital interest as the legal basis do not apply.

b. Vital interest

Vital interest is used as a lawful basis when:

- dealing with emergency situations where the person enquiring about a missing loved one cannot physically and/or psychologically provide any feedback on how personal data will be used by the ICRC and/or the National Society
- providing RFL services is necessary to protect the lives, integrity, health or dignity of beneficiaries.

c. Legitimate interest

Legitimate interest is used as a lawful basis when processing personal data is necessary in order to:

- secure information systems and the related services that are offered by – or are accessible via – these information systems, public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services, and providers of security technologies and services. This could include preventing unauthorized access to electronic communication networks, malicious code and denial-of-service attacks and damage to computer and electronic communication systems, or it could include processing data while scanning IT systems for viruses.
- prevent and provide evidence for fraud or theft, for example, verifying the identity of beneficiaries when they are asking to exercise their rights.
- anonymize or pseudonymize the data.
- establish, exercise or defend legal claims, whether as part of a judicial, administrative or out-of-court procedure, a direct marketing and/or public relations campaign. An example would be the need to defend legal claims made by a beneficiary.
- internally monitor RFL capabilities, including assessing the effectiveness of RFL responses and support and carrying out lessons learned exercises.

d. Compliance with a legal obligation

Depending on the data controller's circumstances, compliance with a legal obligation may include:

- compliance with national or regional legislation, for example in the areas of employment law, financial reporting, fraud, money laundering, etc.
- court orders.

Annex 3: Data security

Personal data should be processed in a way that maintains the confidentiality, integrity and availability of the data. This includes preventing unauthorized access to or use of personal data and the equipment used to process them.

Anybody acting under the authority of the data controller that has access to the personal data shall process them in accordance with the CoC and with the applicable data security policy, which is explained in more detail in this annex.

In order to safeguard data and to prevent breaching this CoC, the data controller shall evaluate the specific risks inherent to the processing and implement measures to mitigate those risks. This assessment should be done in close cooperation with the information security or information technology team, where available, or external consultants, where possible. 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 risks and to the nature of the personal data to be protected. Some of these measures are as follows:

- training
- management of access rights to databases containing personal data
- physical security of databases
- IT security
- data classification
- discretion clauses
- methods of destruction of personal data
- any other appropriate measures.

The objective of these measures is to ensure that personal data are kept safe, in both a technical and organizational sense, and are protected against unauthorized modification, copying, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

Data security measures shall vary depending on several factors, including:

- the type of operation
- the nature and sensitivity of the personal data involved
- the form or format of the data storage
- the environment/location of the specific personal data
- the prevailing security and logistical conditions.

Data security measures should be regularly reviewed and updated to ensure a level of data protection that corresponds to the degree of sensitivity applied to the personal data.

The data controller shall be responsible for:

- setting up an information security management system. To that end, the data controller shall put together and regularly update a data security policy that is based on internationally accepted standards and on a risk assessment. For example, this policy shall include physical security guidelines, an IT security policy, e-mail security guidelines, IT equipment usage guidelines, the Information Handling Typology, a contingency plan and guidelines on destroying documents.
- using the digital tools and procedures made available by the CTA to share personal data within the network to the largest extent possible.
- developing the communication infrastructure and databases in order to preserve the integrity and confidentiality of the data, in accordance with the data security policy.

- taking, in accordance with the present CoC, all appropriate measures to keep the data processed in the data controller's information system safe.

1. Access rights to databases

The data controller is responsible for:

- granting access to databases containing personal data.
- ensuring the tools that enable authorized staff to access databases are secure.
- complying with the security rules referred to in this annex.
- ensuring that staff who have been granted access are able to comply with the present CoC. This includes providing training and ensuring staff members have a confidentiality clause in their employment contracts, which must be signed before access to databases is granted.
- ensuring access is granted on a need-to-know basis.
- keeping a record of the staff members that have access to each database and updating it when necessary, for example, a member of staff role changes and no longer require access.
- keeping, if feasible, a historical log of the staff members that have had access to a database for as long as the data processed by these staff members remains in the database. This is important for accountability purposes.

Staff shall process data within the limits of the processing rights granted to them.

Staff with higher access rights or those in charge of managing access rights may be subject to additional contractual confidentiality obligations.

2. Physical security

The data controller is responsible for:

- setting out security rules defining procedural, technical and administrative security controls to maintain the confidentiality, integrity and availability of databases (whether physical or IT based)[9]
- ensuring that staff are informed of these security rules and that they comply with them
- ensuring that unauthorized staff cannot access storage locations
- developing appropriate control mechanisms to ensure that data are kept safe
- ensuring adequate electrical and fire safety standards are implemented in storage locations
- ensuring storage volumes are kept to a necessary minimum.

3. IT security

The data controller shall:

- set out security rules defining procedural, technical and administrative security controls to maintain the confidentiality, integrity and availability of the information systems used
- develop appropriate control mechanisms to ensure that data are kept safe

[9] E.g. lock your computer when leaving your workstation, do not leave sensitive documents in the printer for a long time and do not leave your passwords publicly available on your desk.

- put specific security rules in place for a part of the IT communication infrastructure, a database or a specific department, if considered necessary.

All email correspondence, both internal and external, containing personal data shall be processed on a need-to-know basis. Recipients of email correspondence shall be carefully selected so as to avoid personal data being published unnecessarily. Private email accounts should not be used to transfer personal data, unless they are the only available tool in an emergency situation.

Remote access to the servers and the use of personal devices for work purposes should comply with the safety standards set out in the data controller's IT security policy. Unless absolutely necessary for operational reasons, the use of coaxial outlets and unsecured wireless connections to retrieve, exchange, transmit or transfer personal data must be avoided.

Any staff handling personal data shall take due care when connecting to the data controller's servers remotely. Passwords must always be protected and staff must check that they have properly logged off of computer systems and that they have closed all their browsers.

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

Keeping personal data related to beneficiaries in a device's local storage should be avoided, unless no other option is available (e.g. it is not possible to access authorized document management and storage platforms[10]) and/or for emergency situations. In any case, such information must be removed from these devices once the intended use has been fulfilled.

Portable devices or removable media should not be used to store documents containing personal data that are classified as being particularly sensitive. If this is unavoidable, personal data should be transferred to appropriate computer systems and database applications as soon as it is practical to do so. If flash memory devices such as USB flash drives and memory cards are used to temporarily store personal data, they should be kept safe and the electronic records must be encrypted. Information should be deleted from portable devices or removable media once it has been stored properly and is no longer needed on those devices.

Effective recovery systems and backup procedures should be in place for all electronic records, and the relevant Information and Communications Technology (ICT) officer should ensure that backup procedures are carried out on a regular basis. Sensitive data will need to be backed up more often than regular data. Electronic records should be automated to allow for easy recovery in situations where it is difficult to carry out backup procedures, for example if there are regular power cuts, system failures or natural disasters.

When electronic records and database applications are no longer needed, the data controller should coordinate with the relevant ICT officer to ensure that they are permanently deleted.

4. Duty of confidentiality and staff conduct

The duty of confidentiality is a key element of personal data security. It involves:

[10] For example, the Family Links Answers (FLA) tool

- all staff and external consultants signing confidentiality agreements[11] as part of their employment/consulting contracts. This goes with the requirement that staff should only process data in accordance with the data controller's instructions.
- all external processors being contractually bound by confidentiality clauses. This goes with the requirement that processors should only process data in accordance with the data controller's instructions.
- all staff and external processors accurately applying the Information Handling Typology according to their confidentiality status.
- ensuring that any requests made by a data subject for their personal data to be processed in a certain way are accurately recorded in the data subject's file, in particular if they would like their data to remain confidential and not to be shared with third parties.

In order to limit the risk of data breaches, only authorized staff shall be in charge of collecting and managing data from confidential sources, as well as accessing documents in accordance with the applicable Information Handling Typology, which classifies all information in terms of its level of confidentiality (e.g. public, internal, confidential, strictly confidential).

Staff should use the Information Handling Typology to attribute levels of confidentiality to the data they process, and they should consult, transmit and use the data in a way that is appropriate for the relevant level of confidentiality.

Staff that originally attributed the levels of confidentiality may modify them at any time, in particular by lowering the confidentiality level if they believe the data no longer requires as much protection.

5. Contingency planning

The data controller is responsible for developing and implementing a plan for evacuating records in case of emergencies.

6. Data destruction methods

When it is decided that personal data no longer needs to be stored, all records and backups should be destroyed or rendered anonymous.

The data destruction method that is used shall mainly depend on:

- the nature and sensitivity of the personal data
- the format and storage medium
- the volume of electronic and paper records.

The data controller should conduct a sensitivity assessment prior to destroying data to ensure that appropriate destruction techniques are used to destroy personal data.

a. Destroying paper records

Paper records shall be destroyed using methods such as shredding or burning, which means they cannot be restored or used again.

A decision may be made to convert paper records into digital records. In this case, once paper records have been converted to electronic format, all traces of paper records should be destroyed,

[11] For example, a Non-Disclosure Agreement (NDA)

unless retention of paper records is required by applicable national law, or unless paper copies need to be kept for archiving purposes.

b. Destroying electronic records

Electronic records should be destroyed by ICT staff because using the standard features on computer systems to remove the records does not necessarily ensure they have been properly deleted.

Upon instruction, ICT staff should ensure that all traces of personal data are completely removed from computer systems and other software, including any backup copies.

Disk drives and database applications should be cleared and all rewritable media, such as CDs, DVDs, microfiches, videotapes, and audio tapes that are used to store personal data should be wiped before being reused. Physical measures of destroying electronic records such as recycling, pulverizing or burning should be strictly monitored.

c. Disposal records

The data controller shall ensure that all relevant contracts of service, MOUs, agreements and written transfer or processing contracts include a retention period. This is the amount of time the personal data are stored for before being destroyed. 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 the time and method of destruction, as well as the nature of the records destroyed, should be kept and attached to project or evaluation reports.

The destruction of large volumes of paper records may be outsourced to specialized companies. In this case, the data controller should ensure that these third parties sign confidentiality agreements and that they are contractually obliged to submit disposal records and data destruction certificates.

7. Other measures

Data security also requires appropriate organizational measures to be put in place internally, including regularly distributing data security rules to all employees, informing them of their obligations under data protection law, especially their obligations of confidentiality.

Each data controller shall assign one or more members of their staff (possibly somebody working in administration or IT) the role of data security officer.

The data security officer shall mainly:

- ensure staff comply with the security procedures set out in this CoC and in its applicable security rules
- update these procedures, as and when required
- conduct further training on data security for staff.

Annex 4: Short DPIA guide

The purpose of a DPIA is to identify, assess and address the specific risks to personal data arising from certain RFL activities. A DPIA should lead to measures to avoid, minimize, or otherwise mitigate these risks. The aim of this DPIA guide is to enable RFL staff to carry out a DPIA. A DPIA template for

RFL activities, providing examples of the types of risks and possible mitigating measures, is available to FLN entities as a separate document.

Here are examples of when you should consider carrying out a DPIA.

- Your organization in the field has been storing its files on CDs and paper. Now you want to introduce a cloud-based storage file system. How will you decide which information is best stored where?
- A tsunami destroys dozens of coastal villages. Thousands of people are reported missing. How much personal information should you collect from the families of the missing people? Should it be a lot or minimal? Should it include sensitive data, such as their DNA, religion and political affiliation?
- The government puts a system in place to centralize all information on the people that are missing following the tsunami. They would like you to provide all the information you have on these missing people. How much personal information should you share in order to help trace these missing people? Under what conditions should personal information be disclosed to the government?
- Another humanitarian organization asks you to share data on people living in a refugee camp. Should you share such data? Under what conditions? What are the consequences of doing so? Will the organization be as careful with personal data as you?
- Your organization is planning to collect biometrics on a large scale, using new technologies that allow you to use fingerprint analysis and facial recognition. What technical safeguards must be put in place? What conditions should be set in the contract with the service provider? Will the beneficiaries be comfortable with providing this information?
- Can you publish pictures of unaccompanied children looking for their relatives online? Can you produce posters of missing children? If so, under what circumstances and conditions?
- A social networking site offers to help you to restore contact between relatives that have been separated after a disaster. How could you cooperate with this site without putting the personal data and the individuals concerned at risk?
- Tomorrow, the ICRC is planning to visit a place of detention where a missing person is allegedly being detained. Considering the urgency of the situation, can you transfer a tracing request or a Red Cross message by email to the ICRC?

In some instances, there may not be sufficient time to carry out a full DPIA, or the complexity, sensitivity, and scale of the processing operation does not require a formal DPIA. Nevertheless, a risk assessment with regard to data protection should always be on the minds of RFL staff (and recorded where possible) when making decisions on transferring data. Hence, RFL staff and volunteers should be aware of the DPIA process and consider the questions below.

A DPIA process typically has the following steps. These steps should be reflected in the DPIA report.

A. Scoping

1. Based on the complexity, sensitivity and scale of the processing operation, determine:

- whether a DPIA is necessary
- who will conduct the DPIA

- who will review and validate the DPIA.

2. In the context of the RFL activity in question, describe how personal data are collected, used, stored and shared. This includes creating a stakeholder map and writing a description of the data flow. The following questions should be considered:

- What is the purpose of the processing?
- What type of personal data is collected, from whom and by whom?
- How is the information collected and further processed?
- How, where and how long is it stored?
- What security measures are in place? Will the data undergo any pseudonymization, cleansing or anonymization to protect sensitive information and/or will data that is not strictly necessary be deleted?
- If external processors are used, who has access to the information?

3. Identify stakeholders that may be able to help. This could be internal stakeholders, such as IT experts, legal advisers, psychologists, programming experts, etc., or external stakeholders, such as other organizations, government agencies, social workers, community leaders, legal guardians, etc. that may be interested in or affected by the data processing analysed in the DPIA.

B. Assessment

4. Identify the potential risks of the processing operation and of non-compliance with this CoC for individuals. If internal and/or external stakeholders have been identified, please discuss and deliberate with them. One way to identify risks is to list the threats and vulnerabilities for all the principles of the CoC and then the risks that arise from these threats and vulnerabilities.

5. Assess the risks in terms of the likelihood and severity of the impact.

6. Identify measures to avoid, minimize or otherwise mitigate risks.

7. Put forward recommendations, such as technical and organizational changes or changes to the overall data protection strategy.

C. Approval and Implementation

8. Ask data protection experts[12] to review the assessment and obtain approval from the staff in charge.[13]

9. Implement the agreed recommendations.

[12] Data protection legal advisors or external consultants
[13] For example, the data protection focal point for RFL, if there is one. Alternatively, the person in charge of RFL activities should approve the DPIA.

10. Update the DPIA if there are changes to the activity.

If a DPIA is carried out, this should be reflected in a report that contains information on sections A, B and C above. Depending on the complexity, sensitivity and scale of the processing operation, a DPIA report (the outcome of a DPIA process) may be very short, or more thorough and detailed. A DPIA report may integrate the template that is available to National Societies.

Annex 5: Controllership and joint controllership

An FLN member, whether it is the ICRC or a National Society, will act as data controller when the following conditions are met:

- It is the sole FLN entity providing an RFL service. For instance, it is the only organization opening a specific tracing case, collecting and sharing Red Cross messages or providing phone calls.
- The ICRC and the National Societies (e.g., the ICRC and one National Society or two or more National Societies) do not share any tracing cases or provide other collective initiatives, partnerships or services.

Two or more FLN members, i.e. the ICRC or National Societies, will act as joint controllers when they work together to establish the purposes and means of the data processing operation. An important criterion is that the processing would not be possible without both parties' participation. Therefore, joint controllership will apply when two or more FLN members are providing a certain RFL service to beneficiaries for which they need to collect and use personal data. For instance, it occurs when they are handling a shared tracing caseload.