International Red Cross and Red Crescent Movement
Family Links Network

Code of Conduct on Data Protection

Version 1.0

November 2015

Foreword

This Code of Conduct (CoC) was drafted by a working group composed of representatives of the Austrian Red Cross (Claire Schocher-Döring), Belgian Red Cross (Flanders) (Axel Vande Veegaete, 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, Katja Gysin) and International Federation of Red Cross and Red Cross Societies (Christopher Rassi) (Working Group). Several other representatives of these organizations also took part in the drafting, discussions, and meetings, making important contributions. The Working Group began discussions on this project in late 2013, and has had several working meetings in Mechelen (April 2014), Brussels (July 2014), Vienna (September 2014), Sofia (November 2014), and London (January 2015), in addition to multiple phone conferences and e-mail exchanges. The CoC was adopted within the Working Group by consensus, incorporating feedback received from many National Societies.

The CoC was deemed necessary due to (1) the many actors of the International Red Cross and Red Crescent Movement (Movement) operating in the Family Links Network , and the need to transfer data within the Movement and to other actors, 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. Users of this CoC must also ensure that they comply with their own national legislation. The CoC is a reference document integrated into the Movement's main set of Restoring Family Links (RFL) guidance. Individual members of the Movement will need to adopt and transpose it into their own standard procedures.

This CoC will provide one tool for all members of the Movement to use with regard to protecting fundamental rights and freedoms of individuals, in particular the right to privacy and the protection of personal data, affected by RFL activities. 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 for RFL cases among each other.

Table of Contents

DEFINITIONS PAGE

International Red Cross and Red Crescent Movement (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 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) are the components of the Movement.

Central Tracing Agency (CTA)

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 – undertakes Restoring Family Links (RFL) activities during armed conflict and other situations of violence, disasters and other circumstances that necessitate a humanitarian response. In line with the 1997 Seville Agreement, its 2005 Supplementary Measures and the RFL Strategy of the Movement 2008 – 2018, the CTA has the lead role within the Movement in all matters related to RFL; it coordinates operations and acts as technical advisor to National Societies.

Data Controller

Data controller means any component of the Movement, which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

Data Processor means a person, public authority, agency or other body which processes personal data on behalf of a data controller.

Data Protection Focal Point for RFL

Data Protection Focal Point for RFL means the person or unit with the responsibility to ensure compliance with the CoC.

Data Subject

Data Subject means a natural person (i.e. an individual) who can be identified, directly or indirectly, in particular by reference to personal data.

To determine whether a person is identifiable, it is necessary to take account of all the means reasonably likely to be used either by the controller or any individual to identify the person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the individual, it is necessary to take into account all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological developments. Personal data does not therefore include anonymous information, which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the Data Subject is not or no longer identifiable. This CoC does therefore not concern the processing of such anonymous information, including for statistical and research purposes.

When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. 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. Numbers, location data, online identifiers (e.g. IP addresses or cookie identifiers) or other specific factors as such should not be considered as personal data if they do not identify an individual or make an individual identifiable.

Family members

Persons considered to be family members are at least:

- children born in and out of wedlock, adopted children and step-children;
- life partners, whether by marriage or not;
- parents, including mothers-in-law, fathers-in-law and adoptive parents;
- brothers and sisters born of the same parents, different parents or adopted.
- close relatives[1]

The definition that can be found in domestic law should also be taken into consideration.

[1] in many socio-cultural contexts, a family may include all those persons who live under the same roof or maintain close relationships among themselves. Thus, the concept of family has to be understood based on societal practice and recognition.

Minors

Every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

Other individuals

Apart from the enquirer and the sought person, RFL activities may concern other individuals, such as other family members, witnesses, neighbours, community leaders, other sought persons, etc.

Personal Data

Personal Data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, audio-visual material, a number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

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

Personal Data Breach

Personal Data Breach means a breach of security leading to the risk or actual accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Process / Processing / Processed

Process / Processing / Processed means any operation or set of operations which 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, dissemination or otherwise making available, or deletion. A transfer of data, within or outside the Movement, constitutes a processing operation.

Processing Milestones

Processing milestones are the key steps in the procedure. These milestones have to be documented by Data Controllers and include:

- date and source of data collection;

- if the legal basis for processing is consent, any limitations to consent expressed by the Data Subject;
- date, type, and outcome of data subject request for the exercise of data subject rights;
- date and recipient of any transfer of data;
- date and means of publication;
- Data Protection Impact Assessment (DPIA) if carried out;
- file closure;
- archiving, if applicable.

Recipient

Recipient means a person, public authority, agency or other body other than the data subject, the data controller or the data processor to which the personal data is disclosed.

Restoring Family Links activities and Restoring Family Links-related activities

Restoring Family Links (RFL) is a generic term describing a range of activities aimed at preventing separation of family members, assisting them in re-establishing and maintaining contact, as well as activities designed to clarify the fate and whereabouts of missing persons.

These activities may be linked to other support services, such as the provision of psychological and psychosocial, legal, administrative and material assistance to families and other individuals affected as well as to resettlement and reintegration programmes and to social welfare services (for details see Annex 1).

RFL Services

National Societies and ICRC Delegations around the world have dedicated personnel within their structure that develops and implements RFL activities and RFL-related activities.

The Family Links Network

When families are separated and people are missing due to armed conflict or other situations of violence, disaster, migration or other humanitarian crisis, everything possible must be done to establish their fate and whereabouts, restore contact between them and, if appropriate, reunite them.

The RFL services of the National Societies and the ICRC form a single worldwide network called the '**Family Links Network'**. The CTA acts as technical adviser to and co-ordinator of this Family Links Network. The strength of this humanitarian network is its worldwide capacity to mobilise staff and

volunteers and to work, according to the same principles and methodology, in areas affected by armed conflicts, other situations of violence, disasters, migration, and other humanitarian crisis and across borders.

More information on the Family Links Network is available on the Family Links website: http://familylinks.icrc.org.

Vulnerable person

Vulnerable person in the context of this CoC means any individual with a diminished capacity to provide a freely given, specific, and informed indication of his/her wishes due either to (i) the emotional and psychological impact of family separation and the humanitarian conditions impacting him/her, or (ii) the complexity of the processing required, making it difficult for him/her to fully appreciate the risks and/or opportunities involved, or a combination of the two.

1. Introduction

1.1 Purpose of this Code of Conduct (CoC)

This CoC sets out the minimum principles, commitments, and procedures that the ICRC, National Societies, and the IFRC RFL personnel 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) allow the seamless flow of personal data needed for RFL activities and (3) protect the fundamental rights and freedoms of the enquirer(s), sought person(s) and other individuals such as witnesses or other family members, related to RFL activities according to 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 data controllers' RFL activities and RFL-related activities (see Annex 1).

1.2.2 Personal Data

This CoC applies to the processing of personal data (including data relating to deceased persons) by the Data Controllers in respect of the enquirer(s), sought person(s) and other individuals related to RFL activities.

1.3 The Family Links Network

The 1949 Geneva Conventions, their 1977 Additional Protocols, the Statutes of the International Red Cross and Red Crescent Movement (the Statutes of the Movement), Resolutions adopted by the Council of Delegates and Resolutions of 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 as auxiliaries to their respective public authorities in the humanitarian field and have a unique role in RFL worldwide. They organize, in liaison with the public authorities, different services to assist the victims of armed conflict, natural disasters and other emergencies for whom help is needed.

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 RFL services of the data controllers do their utmost to avoid harming people by the processing of personal data.

1.4.3 Confidentiality or Rules of Disclosure

Where data subjects that share information with the data controllers in confidence, the data controllers must respect and ensure the protection of this information.

Data controllers comply with all applicable national, regional or international legal obligations, subject to the restrictions outlined in this section 1.4. In determining the applicability of such obligations reference will be made to: (1) any privileges and immunities or waiver of obligations enjoyed by the data controllers in the country or region in question; and (2) any legal protections as derived from 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 of the Family Links Network such as "Restoring Family links – a guide to National Red Cross and Red Crescent Societies"[2], "Assessing Restoring Family Links Needs – Handbook for National Societies and the ICRC", "Restoring Family Links in Disasters – Field Manual" and "Guidelines on Providing Restoring Family Links Services to Persons Separated as a Result of Migration"[3] and the Professional Standards for Protection Work[4].

[2] Under revision

[3] Relevant guidance documents can be found in the Family Links Extranet (under construction)

[4] https://www.icrc.org/eng/resources/documents/publication/p0999.htm

2. Basic Principles for Processing and Data Controller Commitments

2.1 Specified Purpose

At the time of collecting data, the data controller will determine and set out the specific, explicit and legitimate purpose(s) for which data is processed.

Data processing is primarily carried out with the humanitarian purpose to restore family links between people separated as a result of armed conflict, other situations of violence, disasters, migration or other situations requiring a humanitarian response.

Data may be processed for purposes other than those initially specified at the time of collection where the further processing is necessary for a compatible humanitarian purpose, such as RFL-related activities and remains at all times in compliance with all relevant data protection laws (for details, see Annex 1).

2.2 Lawful and Fair Processing

The processing of personal data by the data controller is based on one or more of the following:

- Consent of the data subject;
- Vital interest of the data subject or of other individuals;
- Public interest;
- Legitimate interest of the data controllers;
- Compliance with a legal obligation.

2.2.1 Consent of the Data Subject

Consent as preferred option: Consent of the data subject is the preferred basis for processing of personal data. Consent is to be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, either by a written, oral or other statement or by a clear affirmative action by the data subject signifying their agreement to process their personal data. Consent covers all processing activities carried out for the same purpose. The data subject should receive explanations in simple language as to the following:

- the identity and contact details of the data controller;
- the specific purpose for processing of his/her personal data and an explanation of the potential risks and benefits;

- the fact that the data controller may process his/her personal data for purposes other than those initially specified at the time of collection, if compatible with a specific purpose mentioned above;
- circumstances in which it might not be possible to treat his/her personal data confidentially;
- the data subject's rights and limitations on his/her rights to access, correct and delete their personal data and later object to processing;
- an indication of the security measures implemented by the data controller regarding the data processing;
- that the data controller may need to transfer data to another country; and
- an indication of the data controller's policy on record retention (how long records are kept and any steps taken to ensure that records are accurate and kept up to date)
- whether his/her personal data can be shared with other organizations (including other components of the Movement), with the State authorities in the country of data collection or another country or be publicly disclosed and to approve that their personal data be used as explained.

Consent can be given with limitations. Details of the consent given, the level of confidentiality required, and any applicable limitations are registered and accompany personal data throughout processing.

Alternatives to consent - particularly where consent cannot be obtained/reasonably obtained, personal data is processed on the basis of one of the following:

- vital interest
- public interest
- legitimate interest of the data controller
- compliance with a legal obligation

In such a case, the data controller will, if possible, ensure that the data subject is aware of such processing and is in a position to object to processing if they so wish.

2.2.2 Vital Interest

There is a presumption that the processing of personal data by the RFL services of the data controller, to restore family links, ascertain the fate and whereabouts of missing persons and provide emergency

assistance and protection, is in the vital interest of a data subject or other individuals in certain circumstances, notably:

- when a data subject is being sought by his/her relatives, reported as missing, deprived of liberty, subject to abuses or possibly dead;
- when the data subject is particularly vulnerable and/or not in a position to provide free and informed consent, nor anticipate or understand the risks and benefits of the processing of his/her personal data.

2.2.3 Public Interest

RFL and RFL-related activities of the data controller are in the public interest, as they are exclusively humanitarian as outlined in section 1.3 above. (For examples, see Annex 2)

2.2.4 Legitimate Interest

Personal data is 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 the legitimate interest (for examples, see Annex 3).

2.2.5 Compliance with a Legal Obligation

The data controller will also process personal data in compliance with any applicable legal obligation, such as compliance with national and regional legislation and court orders, 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

The data controller ensures that any person or entity who has access to personal data and acts under its instructions (and is therefore a processor) will not process such personal data except in a manner compliant with this CoC. The data controller also ensures that the responsibilities of each entity involved in processing personal data are clearly allocated and are reflected in appropriate contractual clauses. See section 4 below for further information on transferring data to third parties where it is contemplated that the receiving third party will not process 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 RFL services of the data controller will be kept under review to ensure that it is adequate, relevant and not excessive for the purposes for which it is collected and processed, except when it is archived.

Data accuracy - personal data will be sufficiently accurate, complete and up to date for the purpose for which it is collected and processed.

2.3.3 Data Protection By Design and By Default

Appropriate technical and organizational measures will be taken to meet the requirements of this CoC in designing data management systems and setting up procedures for the collection of personal data.

2.3.4 Data Protection Impact Assessment (DPIA)

Where processing is likely to present specific 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, in consultation with the data subject and other stakeholders, in order to determine and evaluate, in particular:

- 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 minimised and the processing of personal data is in compliance with this CoC and any applicable laws.

The outcome of a DPIA should be a minimisation of risk of harm and/or possible encroachment on the rights and freedoms of the data subject. The data controller will document the outcome and the reasons why that outcome was reached. The data controller will also ensure that steps taken as a result of the DPIA are properly implemented and have the desired effect.

2.3.5 Documentation of Processing

The data controller ensures that electronic/paper records are kept, setting out: (i) databases in which it carries out processing of personal data, and (ii) key data processing milestones. These milestones are recorded in the database/individual file of the data subject.

2.3.6 Data Retention

Personal data will be archived or deleted in accordance with the RFL services data retention policy of the data controller when it is no longer needed for the purposes for which it was collected, for further processing, or for processing on another legitimate/lawful basis (see also Section 3.3).

2.3.7 Data Security

Reasonable technical, physical and organizational security measures will always be taken at any stage of data processing to protect personal data against loss, theft, unauthorized or unlawful access or disclosure. Access to personal data is limited only to personnel of the data controller who require this

access to deliver a specific service or task, with safeguards and access restrictions (for details, see Annex 4).

2.3.8 Personal Data Breaches

The data controller notifies the data subject of the occurrence of a personal data breach if it is likely to affect the rights and freedoms of the data subject.

The purpose of personal data breach notifications to a data subject is to minimize risks of negative effects on the data subject.

The data controller may decide that communication of a personal data breach to the data subject is not required if one or more of the following applies:

- the data controller has implemented appropriate organizational, technological or physical protection 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 subjects rights and freedoms are no longer likely to be severely affected;
- it would involve disproportionate effort, in particular owing to the prevailing logistical or security conditions, or the number of cases involved. In such case, the data controller will instead consider whether it would be appropriate to issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner;
- it would adversely affect a substantial public interest, including the viability of the data controller's operations;
- approaching the data subject, due to the prevailing security circumstances, could endanger the data subject him/herself.

3. Rights of Data Subjects

3.1 Information and Access

When collecting personal data, or as soon as possible thereafter, the data controller will provide the data subject, subject to logistical and security constraints, with information on the processing of their personal data, orally or in writing using the most appropriate means (for a list of the information to be provided, see Annex 5).

Data subjects have the right to obtain at any time, on request, confirmation as to whether or not personal data concerning them is being processed. Where such personal data is indeed being

processed, they are entitled to obtain access to their personal data and information about the purpose of processing, recipients of the personal data and safeguards adopted.

On request, a copy of the document(s) containing their personal data is provided.

This section does not apply if access to data needs to be restricted as a result of:

- overriding public interest
- data protection interests and rights and freedoms of others
- the documents in question cannot be meaningfully redacted

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

3.2 Disclosure to Family Members and Guardians

A request for disclosure of personal data from a family member or legal guardian of a child or other data subject who cannot provide consent due to incapacity is presumed to be in the best interest of that person and therefore granted, unless there is sufficient reason to believe otherwise. The affected person should be consulted, where possible, in order to determine whether they object to such disclosure.

3.3 Rectification and Deletion

Rectification - The data controller will respond to requests to have personal data rectified, in particular if the data is inaccurate or incomplete. The data controller will communicate rectifications carried out to recipients of the personal data, unless the rectification is not significant, or unless communication involves a disproportionate effort.

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

- it is no longer needed for the purposes for which his/her personal data was collected or is not needed for further processing;
- the data subject has withdrawn his/her consent for processing and there is no other basis for the processing of his/her personal data;
- the data subject successfully objects to the processing of his/her personal data;
- the processing of a data subject's personal data otherwise does not comply with this CoC.

However, the continued retention of a data subject's personal data is allowed where this is necessary or justified:

- for historical, statistical and scientific purposes, such as for the purpose of documenting action taken by a data controller in the performance of its mandate under the Geneva Conventions of 1949, the Additional Protocols thereto of 1977, and / or the Statutes of the Movement;
- for reasons of public interest in the area of public health; or
- 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, the continued retention of a data subject's personal data will be allowed where required by law. A data subject will be notified of a decision taken on his/her request, which shall be documented by data controllers.

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 in case deletion would be detrimental to the data subject's vital interests.

The data controller will communicate deletion of personal data to recipients and will request them to erase any links or copies of such data, unless the data erased is not significant or unless communication involves a disproportionate effort.

3.4 Objection to the Processing

A data subject has the right to object, on reasoned grounds relating to his/her particular situation, to processing of his/her personal data that is based on the data controller's legitimate interests or in the public interest. Where the objection is accepted, the concerned personal data will no longer be processed unless the data controller demonstrates overriding legitimate grounds for the continued processing.

Where the objection is accepted, the data controller will communicate such objection to data recipients, unless this involves a disproportionate effort.

3.5 Remedies

A data subject addresses his/her request to the data controller which provides an answer within a reasonable timeframe and in any event within any timeframe imposed by law.

The personnel receiving a request from a data subject will:

- either accede to the request and notify the requesting person how the request was or will be complied with; or
- inform the requesting data subject why the request will or cannot be complied with; and
- inform the data subject of the possibility of bringing a complaint to the data controller.

4. Special provision on Data Transfers

4.1 General Principles

4.1.1 Background

RFL and RFL-related activities often involve the cross-border transfer of personal data between data controllers.

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

These transfers take place in accordance with the activities of the Family Links Network as outlined in Section 1.3; as such they are carried out on important grounds of public interest and per the principles and guidelines of the Movement set out in Section 1.4.

In addition, in most cases these transfers will take place on the basis of consent and/or to protect the vital interests of the data subject or other individuals.

4.1.2 General Principles Applicable to Data Transfers

A transfer of data, within or outside the Movement, constitutes a processing operation. As such, it is subject to the Basic Principles set out in Chapter 2 and the Rights of Data Subjects set out in Chapter 3. Transfers constitute, however, a particularly delicate processing operation. Accordingly, some processing requirements are particularly important such as DPIA, information to the data subject and data security.

As set out in Section 3.1., above, transfer to all reasonably foreseeable third parties is anticipated prior to/at the time of data collection and consent of the data subject to the transfer of their personal data is obtained where possible.

Personal data must not be transferred to people or organizations unless appropriate and proportionate safeguards are put in place, taking into account the sensitivity of the data, the urgency of humanitarian action, and logistical and security constraints, as detailed in this CoC.

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. Accordingly, where transfer of data is likely to present specific risks to the rights and freedoms of data subjects, the data controller will carry out an DPIA (See Annex 6 for guidance) prior to the transfer as set out in section 2.3.4 above.

4.1.4 Conditions

Data transfers are subject to the following, cumulative, conditions:

- Processing by the recipient is strictly limited to the specified purposes of RFL and RFL-related activities and compatible purposes;
- Amount and type of personal data is strictly limited to the recipient's needs for the specified purposes or intended further processing;
- The transfer is compatible with the reasonable expectations of the data subject.

4.1.5 Documentation of Data Transfers

The data controller will ensure that electronic/paper records of transfers are maintained (see also 2.3.5).

Records of transfer should include all of the following:

- name of recipient
- specified purpose of transfer;
- date of transfer;
- description of the categories of personal data that have been transferred;
- any limitations on the use of data agreed upon by the recipient.

4.1.6 Agreements

As set out in section 4.1.2, a transfer of personal data may take place if the data controller has satisfied itself of the existence of appropriate safeguards with respect to the protection of personal data by the recipient. Appropriate safeguards may be established through agreements in respect of the treatment of personal data concluded, where possible, with third parties outside of the Movement whenever regular transfers of data are contemplated.

Even when agreements are obtained, it may not be appropriate to transfer certain categories of data.

4.2 Methods of Transmission

In the event of transfer, appropriate measures will be used to safeguard the transmission of personal data to third parties. The level of security adopted and method of transmission will be proportionate to the nature and sensitivity of 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 2 and the Rights of Data Subjects set out in Chapter 3. Publication constitutes, however, a particularly delicate processing operation. Once published, the data controller and the data subject lose, to a large extent, the capacity to control the way in which personal data is being processed. Accordingly, the additional principles set out in this chapter will also be followed.

Subject to DPIA's and applicable legal obligations, RFL services of the data controller may publish personal data to restore family links between persons separated by armed conflicts, other situations of violence, natural disasters and migration. Such data may include names, pictures, status (such as alive and well, wounded, deceased, missing, displaced) and may be published online, through the media, posters, leaflets or other suitable tools.

In accordance with section 2.2.1, consent of the data subject is the preferred basis for publication of personal data.

5.2 Data Protection Impact Assessment for Data Publication

The requirement to carry out a DPIA, set out in Section 2.3.4 above and Annex 6, is particularly important in the context of data publication.

In addition to the elements set out in Section 2.3.4 "Data Protection Impact Assessment", above, in the context of publication, the DPIA will take into account the following elements:

- 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, if it is necessary to publish personal data, whether other means to protect the identity of data subjects will serve the specified purpose of the publication (such other means may include, for example, not associating a picture with names/distinguishing features/precise locations);

- the method and conditions of publication;
- the possibility of enforcing a requirement to limit further use vis-à-vis third parties that may want to use the published data;
- the possibility of specifying the period during which certain data may remain published on a particular media support, and method of destruction after the specified purpose of publication has been fulfilled;
- the usefulness and appropriateness of the publications through periodic evaluations by the data controller;
- in the context of public communication, the importance of protecting vulnerable persons from public curiosity.

If the data subject is a vulnerable person additional considerations will, where appropriate, be taken into account, including further safeguards to protect confidentiality and anonymity. The guiding principle of victim protection is to "do no harm" and to act in the best interest of vulnerable data subjects.

5.3 Documentation of Data Publication

The data controller ensures a record of publications made is maintained.

Records of data publication include all of the following:

- date of publication;
- if relevant, date on which the basis for publication must be reviewed, in accordance with the DPIA;
- if relevant, date on which data must be removed from publication;
- description of the categories of personal data that have been published;
- where possible, details of media support used.

5.4 Data to be Published for RFL

Data which may be published is to be defined for each given context, and more specific guidance may be available in relation to specific categories of data subjects. Based on the DPIA specific mitigation measures may include the following:

- The publication is limited to the data absolutely necessary to permit the reader/listener to identify the persons whose names/pictures are published and restore contact.
- Pictures of vulnerable people are not published in combination with other personal data (e.g. name), and the address of a minor is never published.

5.5 Data to be Published for Public Archives

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

5.6 Data to be Published for Public Communication

Personal data may be published for purposes of promoting RFL activities, and/or raising awareness about situations of concern, in line with applicable legislation. 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 undertaken.

5.7 Right to Withdraw Consent/to have Published Materials Deleted

Where publication occurs on the basis of consent, at any point, a data subject may withdraw consent for the publication of materials identifying him/her. In this case, the data controller takes all reasonable steps, noting the inherent difficulties with deletion of public documents (particularly online), to withdraw the published materials, and/or to prevent their publication.

Where publication takes place on a basis other than consent, the procedures set out under Section 3.4 "Objection to the Processing" will be followed.

6. Application of the CoC

A CoC application group will support the implementation at a global level of the CoC by advancing continuous learning and development.

The present CoC must be effectively applied by all data controllers, subject to national legislation, as follows:

- The CoC is reflected in RFL policies, guidelines and programmes.
- The CoC becomes an integral part of RFL personnel management and training for each data controller.
- A Data Protection Focal Point for RFL is appointed and contact details shared.
- Participation in periodic surveys on the implementation of this CoC
- Cooperation with the CoC application group.
- Monitoring, which entails self-monitoring, dialogue, peer review and other forms of review, is done voluntarily to ensure continuous improvement and organizational learning.

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

7. References

7.1 Legal Instruments/Guidance

- UN Guidelines for the Regulation of Computerized Personal Data Files, as adopted by General Assembly resolution 49/95 of 14 December 1990;
- Art. 17 International Covenant on Civil and Political Rights;
- International Standard on the protection of personal data and privacy by the International Conference of Data Protection and Privacy Commissioners, 5 November 2009, http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf;
- Convention of the Council of Europe for the Protection of Individuals with regard to Automatic 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;
- Art. 8 European Convention for the protection of Human Rights and fundamental freedoms, 4 November 1950;
- Art. 16 Treaty on the Functioning of the European Union (TFEU), 13 December 2007, *OJ* C 236, 26 November 2012, p. 0001-0390;
- Articles 7 - 8 Charter of Fundamental Rights of the European Union, *OJ*. C 303/1, 14 December 2007;
- Organisation for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (update 2013), oe.cd/privacy;
- OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 9 December 1999, www.oecd.org/sti/consumer/34023811.pdf ;
- APEC Privacy Framework, 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

- Statutes of the International Red Cross and Red Crescent Movement, as amended in 2006;
- Resolution 4 by the Council of Delegates on Restoring Family links Strategy for the International Red Cross and Red Crescent Movement, 24 November 2007;
- International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands, 2015, https://icdppc.org/document-archive/adopted-resolutions/

7.2 Doctrine

- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Restoring family links in disasters: field manual,* Switzerland, ICRC, 2009, 211 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Assessing restoring family links needs: handbook for national societies and the ICRC*, Switzerland, ICRC, 2010, 103 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (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*, Switzerland, ICRC, 2010, 59 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Restoring family links strategy: including legal references*, Switzerland, ICRC, 2009, 64 p.;
- MORGAN, O., TIDBALL- BINZ, M., VAN ALPHEN, D. (*EDS.), Management of dead bodies after disasters: A field manual for first responders*, Washington D.C., 2009, 53 p.;

ANNEXES

Annex 1: RFL Activities and RFL-related Activities

RFL Activities - depending on the situation and the context, may be of different types:

- organizing the exchange of family news;
- tracing individuals;
- registering and following up individuals (children or adults) to prevent their disappearance and to enable their families to be informed;
- reuniting families and repatriation;
- collecting, managing and forwarding information on the dead;
- transmitting official documents, such as birth certificates, identity papers or various other certificates issued by the authorities;
- issuing attestations of individual detention and documents attesting to other situations that led to individual registration;
- issuing ICRC travel documents;
- monitoring the integration of those reunited with their family members;
- promoting and supporting the establishment of mechanisms to clarify the fate and whereabouts of persons unaccounted for;

See also: http://familylinks.icrc.org

RFL-related activities - other humanitarian services related to RFL activities, carried out by RFL personnel:

- Material, legal, psychological and psychosocial support to the families of the missing and other individuals affected by armed conflict, other situations of violence, disasters, migration and other humanitarian crises
- Support to relevant authorities on the management of human remains and forensic identification
- (Referral to) Social-welfare services
- Resettlement services or (referral to) reintegration support services for vulnerable groups
- Archiving (individual/family memory; memory of humanity; individual administrative needs, accountability of the Parties, historical, statistical, and medical research)
- Public communication for the promotion of RFL and RFL-related activities

Annex 2: Public Interest

Examples of Public Interest include:

- When dealing with large-scale crises requiring immediate action, making it not possible to operate on the basis of consent, and it is not possible to establish clearly whether the vital interest legitimate basis applies. One example may be when large numbers of migrants are rescued at sea.
- When the processing operations involved 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, and make a fully informed decision on this basis. Where the vital interests of the data subject or of another individual cannot be established (either due to lack of urgency or because the data subject is being sought) processing can take place on the basis of the mandate of the Data Controller, provided a satisfactory DPIA is carried out.
- Distributions of assistance, where it may not be practicable to obtain the consent of all the possible beneficiaries, and where the life and integrity of the data subject or of other people are reasonably not likely to be at stake (in which case “Vital Interest” may be the most appropriate basis for processing).
- Processing of Personal Data of a data subject in detention. This may happen, for example, when processing Personal Data relating to persons deprived of their liberty in the context of an armed conflict or other situation of violence, where the ICRC (or the National Society) has not yet been in a position to visit the data subject deprived of liberty and obtain their consent and where the prevailing detention conditions in the case in question could rebut the presumption of the “Vital Interest” basis being triggered.

Annex 3: Legitimate Interest

Examples of Legitimate Interest include:

- Processing is necessary for the effective performance of the Data Controller's mandate in accordance with the Fundamental Principles (in particular neutrality, independence and impartiality) and its standard working modalities;
- Processing of data to the extent strictly necessary for the purposes of ensuring information systems and information security, and the security of the related services offered by, or accessible via, these information systems, by public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services and by providers of security technologies and services. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems;
- Processing of Personal Data to the extent strictly necessary for the purposes of preventing, evidencing and stopping fraud or theft;
- Processing of Personal Data for the purposes of anonymising or pseudonymising Personal data;
- where necessary for the establishment, exercise or defence of legal claims, regardless of whether in a judicial, administrative or any out-of-court procedure; direct marketing and/or public communication.

Annex 4: Data Security

Personal Data should be processed in a manner that ensures appropriate security of the personal data, including the prevention of unauthorised access to or use of personal data and the equipment used for the processing.

Any person acting under the authority of the data controller who has access to personal data, shall not process it except in a manner compliant with the CoC and with the applicable Data Security Policy, as further explained in this Annex.

In order to maintain security and to prevent processing in breach of this CoC, the controller shall evaluate the specific risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security (taking into account available technology, prevailing security and logistical conditions, and the costs of implementation) in relation to the risks and the nature of the personal data to be protected. This includes measures involving:

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

The objective of these measures is to ensure that personal data is kept secure, both technically and organizationally, and is protected by reasonable and appropriate measures against unauthorized modification, copying, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer.

Data security measures shall vary depending, among others, on the:

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

Data security measures should be routinely reviewed and upgraded to ensure a level of data protection that is appropriate to the degree of sensitivity applied to personal data.

The data controller shall be responsible for coordinating the following:

- setting up an information security management system. To that end, it shall establish and regularly update a Data Security Policy based on internationally accepted standards and on a risk assessment, and which shall consist of, for example Physical Security Guidelines, IT Security Policy, E-mail Security Guidelines, IT Equipment Usage Guidelines, the Information Handling Typology, a Contingency Plan and Document Destruction Guidelines;
- developing the communication infrastructure and databases in order to preserve the integrity and security of data, in compliance with the security policy established;
- taking, in accordance with the present CoC, all appropriate measures to protect the security of data processed in the data controller's information system.

1. Access Rights to Databases

The Controller is responsible for:

- the granting of access to databases containing personal data;
- the security of the facilities which enable authorised personnel to access that system;
- compliance with the security rules referred to in this Annex;
- ensuring that the personnel being granted access shall be able to observe the present CoC. This includes training, and a discretion commitment in the employment contract signed, before access to databases is granted;
- ensuring access is granted on a "need to know" basis;
- maintaining a register of personnel having access to each database, and updating it when appropriate (e.g. personnel being given different responsibilities that no longer require access);
- if feasible, a historical log of personnel having had access to a database should be kept to ensure accountability, for as long as the data processed by such personnel is present in the database.

Personnel shall process data within the limits of the Processing rights granted to them.

Personnel with higher access rights or in charge of administration of access rights may be subject to additional contractual obligations of discretion.

2. Physical Security

Each data controller is responsible for:

- laying down security rules defining procedural, technical and administrative security controls that ensure appropriate levels of confidentiality, and physical integrity and availability of databases (whether physical or IT based), based on the prevailing risks identified;

- ensuring that personnel are informed of such security rules and complies with them;
- developing appropriate control mechanisms to ensure that the security of data is maintained;
- ensuring adequate electrical and fire safety standards are applied to storage locations;
- ensuring storage volumes are kept to a strict necessary minimum.

3. IT Security

The data controller shall:

- lay down security rules defining procedural, technical and administrative security controls that ensure appropriate levels of confidentiality, integrity and availability for the information systems used, based on risk assessment;
- develop appropriate control mechanisms to ensure that the security of data is maintained;
- establish specific security rules for a part of the IT communication infrastructure, a database or a specific department if it considers it necessary;

All e-mail correspondence, internal and external, containing personal data shall be processed on a "need to know" basis. Recipients of e-mail correspondence shall be carefully selected to avoid unnecessary dissemination of personal data.

Remote access to the servers and the use of home-based desktops or laptops 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 internet outlets and unsecured wireless connections to retrieve, exchange, transmit or transfer personal data must be avoided.

Personnel handling personal data shall take due care when connecting to the data controller's servers remotely. Passwords shall always be protected and personnel shall check that they have logged-off properly from computer systems, and that open browsers have been closed.

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.

Portable or removable devices should not be used to store documents containing personal data, 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 reasonably practical. If flash memory such as USB flash drives and memory cards are used to temporarily store personal data, it should be kept safe and the electronic record must be encrypted. Information should be deleted from the portable or removable device once it has been stored properly, if no longer needed on such support.

Recovery and backup

Effective recovery mechanisms and backup procedures should cover all electronic records, and the relevant Information and Communications Technology (ICT) officer should ensure that backup procedures are done on a regular basis. The frequency of backup procedures shall vary depending on the sensitivity of the personal data. Electronic records should be automated to allow for easy recovery in situations where backup procedures are difficult due to, inter alia, regular power outage, system failure or natural disaster.

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

4. Duty of Discretion and Conduct of Personnel

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

- all personnel and external consultants signing discretion and confidentiality agreements as part of their employment/consulting contract. This requirement goes together with the requirement that personnel should only process data in accordance with the data controller's instructions;
- any external processor being contractually bound by confidentiality clauses. This requirement goes together with the requirement that the processor should only process data in accordance with the data controller's instructions;
- the strict application of the Information Handling Typology based on their confidentiality status; and
- ensuring that any request by data subjects that their personal data be processed in a particular way, and in particular that it be considered confidential and not shared with third parties, is accurately recorded in the file of the data subject.

In order to limit the risk of leaks, only authorised personnel shall be in charge of the collection and management of data from confidential sources, and have access to documents according to the applicable Information Handling Typology;

Personnel are responsible for attributing levels of confidentiality to the data they process based on the applicable Information Handling Typology, and for observing the confidentiality of the data they consult, transmit or use for external processing purposes.

Personnel who originally attributed the level of confidentiality may, at any time, modify the level of confidentiality that it has attributed to data, in particular by attributing a lower confidentiality level than the one previously indicated if it considers that the data requires less protection.

5. Contingency Planning

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

6. Destruction Methods

When it is established that retention of personal data is no longer necessary, all records and backups should be destroyed or rendered anonymous.

The method of destruction shall depend, inter alia, on the:

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

The Controller should conduct a sensitivity assessment prior to destruction to ensure that appropriate methods of destruction are used to eliminate personal data.

Destruction of paper records

Paper records shall be destroyed by using methods such as shredding or burning, which do not allow for future use or reconstruction.

If it is decided that paper records should be converted into digital records, following accurate conversion of paper records to electronic format, all traces of paper records should be destroyed, unless retention of paper records is required by applicable national law, or unless a paper copy should be kept for archiving purposes.

Destruction of electronic records

The destruction of electronic records should be referred to the relevant ICT personnel because the erasure features on computer systems do not necessarily ensure complete elimination.

Upon instruction, the relevant ICT personnel should ensure that all traces of Personal Data are completely removed from computer systems and other software.

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

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 for the destruction of personal data after the fulfilment of the specified purpose. Third parties should return personal data to the data controller and certify that all copies of the personal data have been destroyed, including the personal data disclosed to its authorized agents and subcontractors. Disposal records indicating time and method of destruction, as well as the nature of the records destroyed, should be maintained and attached to project or evaluation reports.

The destruction of large volumes of paper records may be outsourced to specialized companies. In these circumstances the data controller should ensure that the confidentiality of personal data is respected in writing and that the submission of disposal records and certification of destruction form part of the contractual obligations of third parties.

7. Other Measures

Data security also requires appropriate internal organizational rules, including regular internal dissemination of data security rules and their obligations under data protection law to all employees, especially regarding their obligations of confidentiality.

Appointment of a security officer

Each data controller shall attribute the role of data security officer to one or more persons of their staff (possibly Admin/IT) to carry out security operations.

The security officer shall, in particular:

- ensure compliance with the security procedures established by this CoC and in its applicable Security Rules;
- update these procedures, as and when required;
- conduct further training on data security for personnel.

Annex 5: Information to be Provided

Information to be provided :	Consent	Vital Interest/ Public Interest	Legitimate Interest	Contractual/ Legal obligation
Data controller / staff in charge	Yes	Yes	Yes	Yes
Purpose of processing	Yes	Yes	Yes	Yes
Envisaged external processors	Yes	DPIA & privacy disclosure if possible	Yes	Yes
Envisaged transfers	Yes	DPIA & privacy disclosure if possible	Yes	Yes
Data subject rights (information, access, correction, deletion, objection)	Yes	DPIA & privacy disclosure if possible	Yes	Yes
If applicable, whether data provision is a statutory / contractual requirement	Not applicable	Not applicable	Yes	Yes

Annex 6: Short DPIA Guidance

The purpose of a data protection impact assessment (DPIA) is to identify, assess and address the specific risks to personal data arising from certain Restoring Family Links (RFL) activities. A DPIA should lead to measures to avoid, minimise, or otherwise mitigate risks. The aim of this DPIA guide is to enable RFL staff to undertake a DPIA. **A DPIA template for RFL activities**, providing examples of the types of risks and possible mitigating measures, **is available to National Societies as a separate document**.

Here are examples of when you should consider conducting a DPIA.

- Your organisation has been storing its files on CDs and paper. Now you want to introduce central electronic storage of the files. How will you decide which information is best stored where?
- A tsunami sweeps away dozens of coastal villages. Thousands are reported missing. How much personal information should you collect from the families of missing persons? Should it be a lot or minimal? Should it include sensitive information (e.g., DNA, religion, political affiliation)?
- The government puts in place a system to centralize all information on missing persons from the tsunami. It wants you to supply all the information you have on missing persons from that event. How much personal information should be shared with it in order to trace missing persons? Under what conditions should personal information be disclosed to it?
- Another humanitarian organisation 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 organisation be as careful with personal data as you?
- Can you publish pictures of unaccompanied children looking for their relatives on the Internet? Can you produce posters of missing children? Under what circumstances and conditions?
- A social network offers to help you with restoring family links after a disaster. How could you co-operate with this social network without compromising the security of the personal data and of the individuals concerned?
- Tomorrow, the ICRC is planning a visit to a place of detention where a sought person is allegedly located. Considering the urgency, can you transfer a tracing request or a Red Cross Message by e-mail 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 in regard to data protection should always be in RFL personnel's minds (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. <u>Scoping</u>

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 is collected, used, stored and shared. This includes a stakeholder mapping and a description of the information flows (i.e., what information is collected, from whom, by whom; how the information is used; how, where and how long it is stored; whether external processors are used, who has access to the information?).

3. Identify stakeholders to be consulted. This could be internal stakeholders (such as IT expert, legal adviser, psychologist, programme experts…), or external stakeholders (such as other organisations, government agencies, social workers, community leaders, legal guardians…).

B. Assessment

4. Identify risks for individuals arising from the processing operation and risks of non-compliance with the Data Protection Code of Conduct.

5. Assess the risks.

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

7. Propose recommendations.

C. Validation and Implementation

8. Seek review and obtain validation.

9. Implement the agreed recommendations.

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

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

Annex 7: Compliance with a legal obligation

May include depending on the circumstances of the data controller

- Compliance with national or regional legislation, for example in the area of employment law, financial reporting, fraud, money laundering
- Court orders