IFRC Policy on the Protection of Personal Data

Document authorization				
Stakeholder	**Name**	**Position**	**Signature**	**Date approved**
Author	James De France	Senior Legal Adviser		
Author	Lucie Laplante	General Counsel		
Owner	Elhadj As Sy	Secretary General		
Authorizer	Julie Hall	Chief of Staff and Director of OSG		
Authorizer	Anitta Underlin	Under Secretary General, Management		
Authorizer	Jagan Chapagain	Under Secretary General, Programmes and Operations		
Authorizer	Dr. Jemilah Mahmood	Under Secretary General, Partnerships; Ad interim Director, Partnerships and Resource Development		
Stakeholder	Andrew Rizk	Director, Finance and Administration		
Stakeholder	Katherine Hummel	Ad interim Director, Human Resources		
Stakeholder	Sylvia Gil	Director, ITD		
Stakeholder	Pascale Meige	Director, Disaster and Crisis Prevention, Response and Recovery		
Stakeholder	Derk Segaar	Director, Communications		
Stakeholder	Emmanuel Capobianco	Director, Health and Care		
Stakeholder	Cecile Aptel	Director, Policy, Strategy and Knowledge		
Stakeholder	Anthony Garnett	Director, OIAI		

Document Control
This document is subject to change control and any amendments to main versions will be recorded below.

Change History

Version	Date	Notes
1.0	25 March 2019	

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest version available. The latest version which supersedes all previous versions is available on FedNet.

Table of Contents

I. INTRODUCTION

1.1. Introductory Comments

The International Federation of Red Cross and Red Crescent societies (hereinafter the "Federation") collects and processes significant amounts of personal data through its many activities. Protecting personal data is of paramount importance to the Federation, thus the Federation has established a Policy on the Protection of Personal Data ("Policy"). The Policy seeks to protect individuals' right to privacy, while guaranteeing that the Federation is able to collect and use personal data in fulfilling its mandate.

The protection of personal data is context specific; it is not possible to cover every scenario that might arise. For this reason, the Policy outlines high-level best-practices, modeled on leading international data protection instruments.

The Federation is cognizant that simply having a Policy is not sufficient to protect against the risk of misuse or loss of personal data. In coordination with this Policy, the Federation will provide data protection training, information and tools, and will continue its ongoing review and implementation of relevant internal procedures and policies.

The Federation enjoys privileges and immunities in many countries in which it operates. Although the application of this Policy shall be without prejudice to any of the privileges and immunities enjoyed by the Federation, the laws and legal system in the countries where the Federation operates should be considered when evaluating data protection risks to individuals and/or groups.

1.2. Scope

The principles outlined in this Policy apply to the processing of personal data. The Policy does not apply to anonymous information: information that cannot be linked to an identified or identifiable natural person.

Compliance with this Policy is mandatory for any person in the service of the Federation, including but not limited to employees, contracted and national staff members, delegates, and secondees. Where appropriate, interns, volunteers, and consultants are also expected to adhere to the principles and practices outlined in the Policy.

Although this Policy is primarily aimed at the protection of personal data, non-personal data related to groups, such as political or religious beliefs, could put groups of individuals at risk. The principles outlined in this Policy should therefore be used as a guide when collecting or processing information about groups.

1.3. Definitions

For the purposes of this Policy, the following definitions apply:

Data Protection

In the context of this Policy, data protection means a set of principles and practices put in place to ensure that any personal data collected and used by, or on behalf of, the Federation is accurate and relevant, and that the personal data is not misused, lost, corrupted, or improperly accessed and shared.

Personal Data

Personal data is any information that may lead to the identification of a living (identified or identifiable), natural person. Some examples of personal data include: name, email or location data, identification number, gender, marital status, date and place of birth.

Sensitive Personal Data

Sensitive personal data types, including but not limited to health information, religious and political beliefs, biometric and genetic data, are considered special categories of personal data. It should be noted that whether personal data is considered to be sensitive may be heavily dependent on the context.

When personal data is found to be sensitive, additional protections and restrictions should be put in place during collection and processing. Such additional protections may include, but are not limited to, the controls identified for the handling of highly confidential information in the Information Handling Guidelines.

Data Controller

The term Data Controller is used to refer to the person or entity that determines the purposes and means of the processing of personal data. A Data Controller has primary responsibility for the protection of personal data.

In practice there may be more than one Data Controller. It should also be noted that there will be circumstances where a Data Controller is a third party, and the Federation will only be a processor of personal data.

Data Processor

A Processor is the individual or entity that performs one or more processing operations on personal data under instructions from the Data Controller.

Third Party

Third Party is any natural or legal person, public authority, agency or body other than the data subject, the Federation, data controller, or data processor.

Processing of Personal Data

Any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, storage, adaption or alteration, retrieval, use, transfer, dissemination, correction, or destruction.

Data Subject

An individual whose personal data is subject to processing.

Affected persons

Individuals who look to or benefit from the Federation's protection or assistance. This may include any person in the country or local community where the Federation is operating.

Data Protection Officer (DPO)

A Federation staff member who oversees the implementation of this Policy.

Personal Data Breach

Unauthorized access to, or destruction, loss, alteration or disclosure of personal data.

II. GENERAL PRINCIPLES

The Federation's processing of personal data shall be guided by the following general principles.

2.1. Fairness and Legitimacy

Personal data should be processed in a fair and legitimate manner. This means that the Federation will only process personal data where a legitimate basis exists and that data subjects should be provided with easily understandable information related to the collection and processing of their data.

Consent is the preferred legitimate basis for processing personal information. However, in the event that obtaining freely given, fully informed consent is not possible, the circumstances should always be documented.

Under certain circumstances, one or more of the following legitimate bases may be used in addition to, or in lieu of consent.

- Performance of a contract;
- Compliance with a legal obligation to which the Federation is subject;
- Protecting the vital interests of a data subject;
- Carrying out a task in the public interest or in line with the Federation's mandate; or
- Pursuing the Federation's legitimate interests.

When evaluating the legitimate bases applicable to a particular processing operation, special consideration should be given to the vulnerability of the data subject (such as a child) and the sensitivity of the personal data to be collected and processed, noting that what may be considered as ordinary personal information in one context could be considered as highly sensitive in another.

2.2. Information

The Federation should provide data subjects with the following information, in an easily understandable manner, when collecting personal data, or as soon thereafter as possible:

- the legitimate basis for which the data will be processed;
- the intended use of the data;
- the importance of providing accurate, complete information and providing any relevant updates to the information already provided;
- the parties that the personal data might be shared with and where they reside;
- how the data will be stored and when and under what circumstances it will be deleted;
- that data subjects may withdraw consent where consent was the legitimate basis relied upon for processing; and
- whom to contact at the Federation should they have any questions regarding the use of their personal data.

The information listed above may not be provided when the Federation is aware or can reasonably assume that the data subject already has, or has access to the relevant information, and where the provision of such information would be impractical in relation to the benefit to the data subject. Additionally, the above information may not be provided when the Federation's legitimate interest in the non-disclosure of such information outweighs the data subject's rights. In case of any doubt, the DPO may be consulted for guidance.

In addition to this Policy, the Federation has privacy statements on some of its websites and other electronic communications. These privacy statements shall be reviewed for information more specific to the collection and use of personal data in the context of the relevant website or process.

2.3. Purpose Specification

Personal data should be collected and processed for a specified purpose and may typically only be processed for other purposes that are compatible with the original purpose. The Federation may process personal data for additional non-compatible purposes where a legitimate basis exists and after considering the rights of the data subjects and weighing the benefits of such further processing against any potential risks.

2.4. Data Quality and Minimization

Personal data collected should be adequate, relevant, accurate and not excessive considering the specified purpose for which the data was collected. All reasonable steps should be taken to ensure that personal data is updated, when necessary. When inaccurate personal data is identified, it should be corrected or deleted without undue delay.

2.5. Data Retention and Disposal

Personal data, whether stored on paper or electronically, should be kept no longer than is necessary to fulfill the specified purpose for which the data are processed. Retention schedules should be maintained by the Library and Archive Services and implemented by each Federation office, division, department or team, based on the anticipated continuing need for the relevant personal data and in accordance with the Information Management Policy and the relevant Records Classification and Disposal Schedule. The DPO may be consulted for guidance regarding retention.

Personal data should be disposed of in accordance with any applicable Federation policy (for instance, the Information Classification Policy and accompanying Guidelines). Information Technology Department (ITD) should be consulted for assistance with secure disposal and electronic file deletion.

2.6. Confidentiality and Security

All stages of personal data processing shall be done in a manner that ensures the appropriate security and confidentiality of personal data. In particular, personal data must be kept secure and protected against data breaches.

It is particularly important to review the adequacy of any security measures during the design phase of any project that involves the processing of personal data so as to ensure that adequate security is in place throughout the project.

The Federation shall routinely review data security measures and upgrade them, as necessary, to ensure an adequate level of data protection with respect to the degree of sensitivity of the personal data.

III. DATA SUBJECT RIGHTS

3.1 Subject to Sections 3.2 and 3.3, data subjects shall have the following rights. The Federation will ensure that a formal mechanism is in place to allow a data subject to exercise his or her rights by making a corresponding request.

3.1.1 Information on Processing

A data subject shall have the right to request information regarding whether his or her personal data has been, is being, or will be processed, by the Federation. The data subject shall further have the right to know the specified purpose(s) for the processing of his or her data.

3.1.2 Access to and Correction of Personal Data

A data subject shall have the right to review his or her personal data for accuracy, completeness and relevance.

When inaccurate or incomplete data is identified, the Federation shall correct and complete the relevant personal data in a timely manner.

3.1.3 Objection to Processing

A data subject has the right to object to the processing of his or her personal data at any time. If the objection is justified, the Federation shall no longer process the personal data concerned for the purpose(s) related to the objection.

3.1.4 Request for Deletion

A data subject may request that his or her personal data be permanently deleted by the Federation. If the request is found to be justified, the Federation should follow any relevant security policies for the secure deletion of paper and electronic data.

3.2 Modalities of Requests Regarding Personal Data

A request to exercise any of the rights listed in Section 3.1 should be made in writing, whenever possible, to the DPO. The request must contain a clear explanation of what is being requested (for example, whether it is a request for correction or objection) and contain sufficient reasoning and evidence to allow the Federation to act upon the request.

If the request is unclear, or the information provided is insufficient, additional information may be requested.

Any request must be accompanied by the requestor's contact information and sufficient documentation to show that the party making the request is the data subject or his or her legal representative or guardian. Where such documentation is not considered sufficient, additional documentation may be requested.

It is recognized that affected persons may not be in a position to address the DPO directly. For this reason, Federation staff, should facilitate such requests, as appropriate.

3.3. Responses to Requests

In all cases, a timely response shall be provided to the data subject (or his or her legal representative) in a manner that is understandable to the data subject.

However, there are a number of circumstances where a request may not be acceded to, and only a limited response will be provided. For instance, where:

- there are grounds for believing that the request is abusive or fraudulent;

- the request is unclear, and/or the reasoning contained in the request is not supported by facts;

- acceding to the request places one or more individuals at risk;

- complying with the request proves to be impossible, inappropriate, or would involve a disproportionate effort when balanced against the data subject's right;

- the request is in conflict with the overriding operational needs and priorities of the Federation in pursuing its legitimate interests;

- the processing of the personal data is necessary for archiving or statistical purposes in the public interest, to protect freedom of expression; or

- the processing of the personal data is necessary for the compliance with a legal obligation or the establishment, exercise or defense of legal claims.

IV. COMMITMENTS

4.1 Data Protection Impact Assessments (DPIA)

The Federation shall conduct a DPIA when processing operations appear likely to result in a high risk to the rights or freedoms of a data subject. Additional guidance will be prepared on when DPIAs are necessary and how to conduct them. In general, a DPIA should contain a description of the project, system, policy or arrangement for the processing and/or sharing of personal data; an analysis of the associated risks; and the measures proposed or already in place to safeguard the personal data according to this Policy.

The following are examples of scenarios when a DPIA might be undertaken, in coordination with the DPO:

- new technology is being used to process personal data;

- individuals may be subject to automated decision making or profiling;

- it is proposed to transfer personal data to a third party who may not be able to ensure adequate safeguards for the protection of the data;

- special categories of personal data, such as health status or religious or political views are involved; or

- mass surveillance or data collection or sharing is envisaged.

4.2 Data Breaches

Although the Federation undertakes to have the best available data security in relation to the risks of a data breach, no security measure (whether technical, physical or organizational) is 100% guaranteed to prevent a breach. It is therefore not only important to provide adequate security, but to also have a reliable method for detecting any security breaches and acting on them quickly.

4.2.1 Notification of a Personal Data Breach to the DPO

In the event of a personal data breach, ITD, or the relevant office, department, unit, entity or individual who detected the breach shall report it to the DPO (and any relevant Federation manager, as specified in the Acceptable Use Policy) without undue delay. The following information should be provided to the DPO:

-how the breach was discovered and when;

-the nature of the breach, the categories of personal data affected, and the estimated number of data subjects concerned;

-the possible consequences of the personal data breach; and

-any measures taken or proposed to be taken to address the breach.

ITD should also be informed and kept closely involved at all stages and in all measures taken in relation to any personal data breach. The Communications Department shall also be informed of any breach at the earliest stage possible.

4.2.2 Notification of a Personal Data Breach to the Data Subject

Based on consultations with the DPO and other relevant office, department or unit, as necessary, if it is determined that a data breach poses a high risk to the rights or freedoms of data subjects, the Federation shall make all reasonable efforts to inform the affected data subjects of the nature of the breach and the measures taken to address it.

4.3 Accountability

The Secretary General is accountable for the implementation of this Policy.

4.3.1 Roles and Responsibilities

In addition to the roles outlined below, other roles may be defined, and/or more detailed guidance provided, in future standard operating procedures and guidelines.

Managers

Managers are responsible for ensuring the workforce under their direction have knowledge of, and handle personal data in accordance with, the data protection principles outlined in this Policy. When appropriate, managers shall also take responsibility for elevating data protection queries and concerns to the DPO.

Data Protection Officer (DPO)

The Federation shall designate a DPO who will serve as the focal point for all data protection matters.

The DPO shall have the following principal responsibilities:

-providing guidance on the application and interpretation of this Policy;

-providing advice on compliance with this Policy and making recommendations on, or updates to, relevant Federation policies or practices, as necessary;

-assisting Federation offices, departments and units with questions related to the design of projects that will process personal data in order to consider any risks (DPIA);

-working to ensure that data protection is considered throughout all stages of a project (Data Protection by Design and by Default); and

-reviewing agreements related to personal data and advising on data protection questions in general.

When appropriate, the DPO may consult with any relevant stakeholder regarding the implementation of this Policy. Such stakeholders include, but are not limited to, the Ombudsperson, ITD, and the General Counsel.

General Counsel

The General Counsel shall be responsible for managing the Federation's legal risk in relation to data protection and for ensuring that the commitments taken by the Federation are in line with the Policy.

Information Technology Department (ITD)

ITD shall have overall responsibility for the maintenance and security of the Federation's information technology resources.

4.3.2 Documentation

To demonstrate compliance with the Policy, detailed, accurate records of personal data collection and processing activities should be maintained.

V. PERSONAL DATA TRANSFERS

Whether it is transferring staff data to a payroll provider or sharing details of affected persons with cash assistance partners, data transfers are a regular and necessary part of the functioning of the Federation and the assistance it provides around the world. However, with each transfer comes the risk of misuse or unauthorized disclosure of the data.

5.1 Transfers to Third Parties

All proposed transfers of personal data to third parties should be reviewed for compatibility with the general principles outlined in Section II of this Policy. Additionally, personal data transfers should only be made to third parties when the third party provides adequate safeguards to protect data and only after the conclusion of a written agreement.

At a minimum, written transfer agreements should require the third party to:

-use the transferred personal data only for the purpose(s) specified in the relevant contract, and more generally only according to the Federation's instructions;

-return to the Federation and/or destroy, as specified, the transferred personal data at the end of the provision of services or at any time upon the Federation's request, for instance to comply with a data subject's request that personal data be deleted;

-implement sufficient security safeguards to prevent unauthorized alteration or loss of, or access to, personal data (these safeguards should include access restrictions, encryption of the data at rest and during transfer, secure storage, and other measures, as appropriate);

-not undertake any onward transfers to other third parties unless expressly agreed to by the Federation;

-only subcontract work with the Federation's consent; and

-promptly notify the Federation in the event that a security incident (breach) occurs.

Given the diverse political and legal environments in which the Federation operates, special attention should be given to the legal framework and enforceability of written agreements/contracts in the relevant region(s).

Finally, it is recognized that it may not be possible to conclude a written agreement prior to sharing personal data with certain partners and in certain exigent circumstances, such as a humanitarian emergency. In such circumstances, and where transfers are necessary to protect affected persons' vital interests, all steps should be taken, as soon as possible after the emergency, to protect the transferred data, including pursuing a written agreement.

5.2. Transfers to Investigative Bodies or Governmental Authorities

Under certain circumstances, the Federation may transfer personal data to certain investigative bodies or to a governmental authority, including law enforcement agencies and courts. Such transfers may be upon request, or on the Federation's own initiative.

The Federation may only cooperate with such a request and transfer personal data if the receiving party agrees to the conditions set out in Section 5.1 and the following conditions are met:

-the Federation received a governmental request through official channels and considers it to be legally valid, or the Federation has concluded a written agreement with the requesting party; and

-the transfer is necessary for the purposes of the detection, prevention, investigation, or prosecution of a criminal offence or violation of the Federation's rules and regulations; and

-the transfer could substantially assist the requesting party in the pursuit of these purposes; and

-the transfer will be limited to the personal data strictly necessary to fulfill the purpose; and

-the transfer does not disproportionately interfere with an individual's fundamental rights.

The DPO shall be consulted prior to entering into any agreement to transfer personal data pursuant to this Section.

VI. CONTACT INFORMATION

For any questions with regard to this Policy or its implementation, please email: [dataprotection@ifrc.org]