ICRC RULES ON PERSONAL DATA PROTECTION

REFERENCE

ICRC

Adopted by the Directorate of the ICRC on 24 February 2015 (updated on 10 November 2015)
Updated and adopted by the ICRC Assembly on 19 December 2019

TABLE OF CONTENTS

PREAMBLE

BACKGROUND

Data protection legislation has been developing rapidly in recent years: around 120 countries now have laws on data protection or some kind of statutory requirement concerning privacy; and new laws continue to be drafted as awareness of the need to protect data spreads throughout the world.

As new technologies are developed and the world is increasingly interconnected, making it possible to process ever increasing quantities of data faster and more easily, the potential for intrusion into individuals' private sphere becomes more significant. This has not gone unnoticed and efforts are being made throughout the world to respond to the issue.

The ICRC recognizes the immense potential of these developments for its humanitarian action, and seeks to incorporate them in its activities. But it is also keenly aware of the risks involved, and of the importance of developing appropriate data protection standards and putting them into effect.

Safeguarding the Personal Data of individuals, particularly in testing conditions such as armed conflicts and other humanitarian emergencies, is an essential aspect of protecting people's lives, their physical and mental integrity, and their dignity – which makes it a matter of fundamental importance for the ICRC. It touches all areas of the ICRC's activity, whether operational or administrative.

As a result, the ICRC has adopted the following set of rules for protecting Personal Data, which will also enable it to remain at the forefront of international humanitarian action, even in the most challenging circumstances.

PURPOSE

These rules are intended to ensure that the ICRC can carry out its mandate under international humanitarian law (IHL) and the Statutes of the International Red Cross and Red Crescent Movement (Statutes of the Movement) in a manner consistent with internationally recognized standards for protecting Personal Data.

They apply solely to the Processing of Personal Data. Defined terms – listed in the annex – appear in capital letters throughout these rules.

THE ICRC'S MANDATE FOR PROCESSING PERSONAL DATA

The ICRC's primary mandate for Processing Personal Data derives from IHL and the Statutes of the Movement, which entrust it with the mission to protect and assist people during armed conflicts and other situations of violence.

The ICRC carries out the activities under its humanitarian mandate in full conformity with its Fundamental Principles – particularly the principles of humanity, impartiality, neutrality, and independence – and in accordance with its standard working methods, especially confidentiality.

To safeguard the neutrality, impartiality and independence of the ICRC's action – and in keeping with the exclusively humanitarian nature of such action – Personal Data Processing by the ICRC is governed exclusively by the present rules and independently supervised by the ICRC Data Protection Office; and effective remedies are ensured through the ICRC Data Protection Independent Control Commission.

P. Moore/ICRC

CHAPTER 1
BASIC PRINCIPLES

ARTICLE 1: LAWFUL AND FAIR PROCESSING

1. The ICRC processes Personal Data based on the principles set out in this chapter.

2. The ICRC shall process Personal Data only if there is a lawful basis for doing so in these rules. The legitimate bases that may apply are the following:
   a. consent of the Data Subject
   b. vital interest of the Data Subject or of another person
   c. public interest, in particular based on the ICRC's mandate under IHL and/or the Statutes of the Movement
   d. legitimate interests of the ICRC, provided that these interests are not overridden by the rights and freedoms of the Data Subjects
   e. performance of a contract
   f. compliance with a legal obligation.

3. Wherever possible, Consent is the preferred basis for Processing Personal Data. However, because of the vulnerability of most of the beneficiaries of ICRC activities, and the nature of the organization's work in humanitarian emergencies, the ICRC may not be in a position to rely on this preferred basis for many of its Processing operations.

4. The ICRC takes particular care in Processing the Personal Data of certain vulnerable categories of Data Subject, such as children, the elderly, mentally disabled people or people who have been psychologically traumatized. The ICRC also takes particular care when processing Personal Data that might cause significant harm to Data Subjects if mishandled. Data of this kind may vary from one context to another, but there is a presumption that health-related Personal Data and biometric data belong to this category.

ARTICLE 2: TRANSPARENT PROCESSING

1. Data Processing must be transparent to the Data Subjects involved. Data Subjects must be given a certain minimum amount of information about the Processing. The ICRC Staff in Charge will decide how this information is to be communicated, after taking into account such matters as security conditions in the field, logistical constraints, and the urgency of the Processing.

2. In addition, all information and communication concerning the Processing of data must be accessible and easy to understand; and clear and plain language should be used.

3. The minimum information to be provided is described in detail in Article 7 below.

ARTICLE 3: PROCESSING FOR SPECIFIC PURPOSES / FURTHER PROCESSING

1. When collecting data, the ICRC Staff in Charge determines the specific and legitimate purpose/s for which data are processed; the data are then processed only for those purposes. Purposes for Processing Personal Data that are within the ICRC's mandate include:
   a. restoring family links
   b. protecting individuals in detention
   c. protecting the civilian population
   d. building respect for IHL – including through training and capacity building
   e. providing medical assistance
   f. forensic activities
   g. weapon decontamination
   h. ensuring economic security
   i. protecting water and sanitation systems
   j. preventive and curative health care.

2. The ICRC may also process data in connection with any other activity necessary to carry out its mandate.

3. The ICRC may process Personal Data for purposes other than those specified at the time of collection if such further Processing is compatible with those original purposes, and, in particular, where the Processing is necessary for historical, statistical or scientific purposes, or accountability of humanitarian action.

4. However, further Processing is not permissible if the risks for the Data Subject outweigh the benefits of further Processing.

ARTICLE 4: ADEQUATE AND RELEVANT DATA

1. The data handled by the ICRC must be adequate and relevant to the purposes for which they are collected and processed.

2. This requires, in particular, ensuring that the data collected are not excessive for the purposes for which they are collected and for compatible further Processing, and that the period for which the data are stored, before being anonymized or archived, is no longer than necessary.

ARTICLE 5: DATA QUALITY

1. Personal Data must be as accurate and up-to-date as possible.

2. Every reasonable precaution must be taken to ensure that Personal Data proven to be inaccurate are corrected or deleted without undue delay (taking into account the purposes for which they are processed).

ARTICLE 6: RETENTION, DELETION, AND ARCHIVING OF DATA THAT ARE NO LONGER NEEDED

1. In order to ensure that data are not kept longer than necessary, a minimum retention period is set, at the end of which a review is carried out to determine whether the data are still required. Depending on the findings of the review, the retention period is renewed or the data are deleted or archived.

2. Personal Data must be deleted when:
   a. they are no longer necessary for the purposes for which they were collected or otherwise further processed
   b. the Data Subjects withdraw their Consent for Processing
   c. the Data Subjects object to the Processing and their objections are upheld by the ICRC Staff in Charge or the ICRC Data Protection Independent Control Commission (Data Protection Commission)
   d. these rules otherwise provide for deletion.

3. However, data should not be deleted when there is a legitimate reason for archiving them: for instance, the data may be necessary for ensuring long-term provision of humanitarian services, or for historical, statistical or scientific purposes, or for accountability of humanitarian action.

T. Gassmann/ICRC

CHAPTER 2
RIGHTS OF DATA SUBJECTS

ARTICLE 7: INFORMATION

1. The following minimum information about data Processing must be provided to Data Subjects – orally or in writing, and in plain and understandable language – when Personal Data are obtained or collected:
   a. whether the ICRC is the Data Controller, and whether there are other Data Controllers
   b. the basic elements of the ICRC's mandate and, if applicable, that of other Data Controllers
   c. the purpose(s) for which data are processed
   d. whether the data are likely to be shared with one or more National Red Cross or Red Crescent Societies and/or other entities
   e. that they may address any questions/concerns/complaints about the handling of data to, first, any ICRC staff member and, second, to the Data Protection Officer or directly to the ICRC Data Protection Commission
   f. the duration of the retention period.

If the ICRC is unable – because of logistical or security constraints – to provide this information when Personal Data are obtained or collected, it must do so at a later date and without any unreasonable delay.

2. When data are not collected directly from the Data Subject, such information must be provided within a reasonable period, orally or in writing, depending on the logistical or security constraints to which the ICRC is subject. It is essential, in every case, to ensure that the information provided to Data Subjects does not cause any harm, prejudice, or distress to them.

ARTICLE 8: ACCESS

1. Data Subjects must be given an opportunity to obtain, on request, at reasonable intervals and without excessive delay, confirmation of the processing of Personal Data relating to them. The data that have been processed should be communicated to them in an intelligible form. Data Subjects should also be able to verify their Personal Data and given access to the data, except in the circumstances listed in paragraph 3 below.

2. Disclosure of Personal Data should not be automatic. The ICRC Staff in Charge should first consider all the circumstances surrounding the request for access and any restrictions to access that may be applicable. ICRC staff should not reveal any information about Data Subjects, unless they are provided with sufficient proof that the person asking for the information is the Data Subject.

3. The right to access documents does not apply when important public interests require that access be denied. These interests include:
   a. upholding confidentiality, a crucial working method for the ICRC
   b. ensuring the viability of operations being carried out under the ICRC's mandate
   c. preserving the confidentiality of ICRC staff members' views or line of reasoning, which, if breached, might jeopardize ICRC operations and/or disclose Personal Data of staff members
   d. the rights and freedoms of others that override the data protection interests of the Data Subject.

4. Requests from parents and legal guardians should be premised on the best interests of the child or vulnerable Data Subject; there is a presumption that access is in the best interest when conducted by the parents and legal guardians. The ICRC Staff in Charge may, however, refuse to reveal Personal Data relating to children if he or she has sufficient reason to believe that it would not be in the best interests of a particular child.

5. It is legitimate for people to seek to reunite their families, to enquire about the whereabouts and well-being of Data Subjects who are their relatives, or to conduct research into their family's history, particularly when separation is due to armed conflicts and other situations of violence. Requests for data for these reasons are legitimate, but they must be weighed against the confidentiality of Personal Data and the rights and interests of Data Subjects.

6. Access to Archived Data is subject to strict conditions and procedures, which are set out in the Rules on Access to the ICRC Archives.

ARTICLE 9: CORRECTION

At the request of a Data Subject, mistakes or inaccuracies in his or her Personal Data must be corrected by the ICRC Staff in Charge, except when:

a. the identity of the Data Subject cannot be verified by the ICRC Staff in Charge
b. the correction request relates to an assessment carried out by ICRC staff, and the Data Subject is unable to provide sufficient proof of the assessment's inaccuracy
c. the data are contained in a record held by the ICRC's archives. In this case, a note may be included in the relevant archive file to indicate that a correction request has been made.

ARTICLE 10: DELETION

1. A Data Subject must be able to have his or her Personal Data deleted from the ICRC's Active Databases when retention of such data is not in compliance with these rules.

2. However, the right to deletion does not apply, and Personal Data will continue to be retained, in the following circumstances:
   a. when the ICRC Staff in Charge is concerned that the Data Subject is requesting deletion because of external pressure, and that deleting Personal Data would harm that Data Subject's vital interests or those of another person

b. for reasons connected to the right to freedom of expression/freedom of information, including for the purposes of documenting the activities of the ICRC in line with the organization's policy of confidentiality
c. when it serves the public interest to do so
d. for historical, statistical and scientific purposes
e. for long-term humanitarian purposes or to establish accountability
f. for the establishment, exercise or defence of legal claims.

ARTICLE 11: OBJECTION

1. Data Subjects may object at any time, on compelling legitimate grounds relating to their particular situation, to the Processing of Personal Data concerning them.

2. An objection of this kind will be accepted if the fundamental rights and freedoms of the Data Subject in question outweigh the ICRC's legitimate interests, or the public interest, in Processing.

ARTICLE 12: PROFILING

The ICRC Staff in Charge shall not take a decision based solely on Profiling (meaning, in this case, any form of automated Processing of Personal Data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict that natural person's performance at work, economic situation, location, health, reliability or behaviour) where such a decision produces legal effects concerning a Data Subject and/or severely affects him or her, unless such Processing is carried out with the Data Subject's Consent.

ARTICLE 13: ASSERTION OF DATA PROTECTION RIGHTS BY INDIVIDUALS

1. Data Subjects may make a formal assertion of their data protection rights with the ICRC Data Protection Office, directly or through any ICRC staff member.

2. When it cannot settle an individual complaint itself, the ICRC Data Protection Office must refer the matter to the ICRC Data Protection Commission.

3. If the Data Protection Office fails to refer the matter to the Data Protection Commission, Data Subjects may also make a formal assertion of their data protection rights directly with the Data Protection Commission.

4. If a complaint is found to be justified, appropriate measures must be taken.

ARTICLE 14: DEROGATIONS

If the ICRC's humanitarian mandate – to protect and assist people affected by armed conflicts and other situations of violence – or its independence, impartiality, or neutrality is threatened, or if the effective performance of ICRC activities is likely to be interrupted, the Directorate of the ICRC may, with regard to data Processing, take temporary measures necessary and appropriate in these circumstances after consultation with the ICRC Data Protection Office and the director of the ICRC Department in charge.

N. Kero/ICRC

CHAPTER 3

ICRC COMMITMENTS

ARTICLE 15: RESPONSIBILITY/ACCOUNTABILITY

1. It is the responsibility of the ICRC Staff in Charge to ensure that everyone with access to Personal Data, and under the authority of the ICRC, handles or processes data in compliance with these rules and with data protection policies accepted by the Directorate.

2. This requires that when the ICRC cooperates with another entity in Processing data, the responsibilities of all parties concerned must be defined very clearly and set out in a contract or other legally binding arrangement. For example, an entity that sets out to Process Personal Data on behalf of the ICRC, the data Processor, must agree to provide certain forms of protection for the data, and agree also to process the data only as directed by the ICRC. If this is not possible, and if the ICRC Staff in Charge takes the view that Processing should take place anyway, the fact should be taken into account in the Data Protection Impact Assessment (see Article 17).

ARTICLE 16: DATA PROTECTION BY DESIGN AND BY DEFAULT

1. While designing a database, data processing, and drafting procedures for collecting Personal Data, all these rules must be taken into account and incorporated to the greatest extent possible; this is known as "data protection by design and by default."

2. Any ICRC Staff in Charge who wishes to create or modify a database must, when that involves the Processing of Personal Data, submit a proposal in this regard to the ICRC Data Protection Office.

ARTICLE 17: DATA PROTECTION IMPACT ASSESSMENTS

1. When data Processing is likely to involve specific risks to the rights and freedoms of Data Subjects, the ICRC Staff in Charge will be responsible for conducting, before the Processing, an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (Data Protection Impact Assessment); during emergencies, this may be done after the Processing, but as soon as reasonably possible.

2. The Data Protection Impact Assessment must make use of standardized forms and guidelines prepared by the ICRC Data Protection Office. It will serve as the basis for the mitigating measures that may have to be implemented. The ICRC Data Protection Office must be consulted; it may give directions on the mitigating measures to be taken, and provide guidance for their implementation.

ARTICLE 18: DOCUMENTATION OF PROCESSING

In order to demonstrate compliance with these rules, the ICRC Data Protection Office maintains records on the categories of Processing activity within its remit, as established and updated by the Staff in Charge.

ARTICLE 19: COOPERATION WITH SUPERVISORY AUTHORITIES

1. Any cooperation with national or regional data protection authorities is always without prejudice to the ICRC's privileges and immunities under domestic and international law. In order to fully protect Data Subjects' Personal Data, the ICRC must ensure that its specific status is recognized and that all parties concerned are aware that the ICRC cannot be compelled to disclose any information acquired while carrying out its work. More specifically, the ICRC's privilege of non-disclosure must be respected.

2. Any request by a data protection supervisory authority for cooperation with the ICRC, or for information on any ICRC Data Subject, must be referred to the ICRC Data Protection Office before it is acceded to.

ARTICLE 20: DATA BREACHES

1. Any breach of security leading to the accidental or unlawful destruction, loss or alteration of – or to the unauthorized disclosure of, or access to – Personal Data transmitted, stored or otherwise processed must always be reported to the ICRC Data Protection Office.

2. The persons affected must be notified of a Data Breach by the Staff in Charge, in close coordination with the Data Protection Office, without undue delay when the Data Breach puts them at particularly serious risk, unless:
   a. that would involve disproportionate effort, owing to logistical circumstances or security conditions, or the number of cases involved. In such cases, the ICRC Staff in Charge, in close coordination with the ICRC Data Protection Office, must consider whether it would be appropriate to issue a public statement or take some similar measure whereby the Data Subjects are informed in an equally effective manner
   b. it would adversely affect a matter of substantial public interest, such as the viability of ICRC operations
   c. approaching the Data Subjects, because of the security conditions, could endanger them or cause them severe distress.

ARTICLE 21: DATA SECURITY

1. Personal Data must be processed in a manner that ensures an appropriate degree of security. A number of factors will be taken into account to determine the level of security required, but particular attention will be paid to these: the nature of the data and the risks to both Data Subjects and the ICRC's mandate. This includes prevention of unauthorized access to or use of Personal Data and the equipment used for data Processing. This relates in particular to access rights to databases, physical security, computer security or cyber security, the duty of discretion and the conduct of staff.

2. When retention of Personal Data is no longer necessary, all records and backups must be securely destroyed or anonymized.

D. Revol/ICRC

CHAPTER 4
DATA TRANSFERS

ARTICLE 22: REQUIREMENTS FOR DATA TRANSFERS

1. Data may be transferred to entities outside the ICRC only when the following conditions have been met:
   a. the identification of an applicable lawful basis for the transfer:
      i. consent of the Data Subject
      ii. vital interest of the Data Subject or of another person;
      iii. public interest, in particular based on the ICRC's mandate under IHL and/or the Statutes of the Movement
      iv. legitimate interests of the ICRC, provided that these interests are not overridden by the rights and freedoms of the Data Subjects
      v. performance of a contract
      vi. compliance with a legal obligation.
   b. a risk assessment is undertaken and appropriate mitigation measures implemented pursuant to Article 23. Depending on the sensitivity of the transfer and the risks it presents to individuals or to the ICRC, it may be necessary to carry out a full Data Protection Impact Assessment in connection with the Personal Data to be transferred.
   c. processing by the Recipient is restricted as much as possible to the specific purposes of ICRC Processing or permissible further Processing.
   d. the amount and the type of Personal Data to be transferred is strictly limited to the Recipient's need to know for the specified purposes or for intended further Processing.
   e. the transfer is not incompatible with the reasonable expectations of the Data Subject.
   f. appropriate measures are used to safeguard the transfer of Personal Data to third parties. The means of transmission, and the security methods employed, must be proportionate to the nature and sensitivity of the Personal Data, the risks revealed by the risk assessment and the urgency of humanitarian action.
   g. a record of the transfer is maintained.

ARTICLE 23: DATA TRANSFER AGREEMENTS

1. For systematic or large-scale Data Transfers, or when the data to be transferred is particularly sensitive – and depending on the urgency of the Processing – a formal agreement between the Recipient and the Data Controller is required. This may be done via dedicated contractual clauses on data security and data protection in a partnership agreement or memorandum of understanding, or in the form of a dedicated Data Transfer agreement.

2. For Data Transfers not subject to such agreements, the following measures must be implemented:
   a. a written undertaking from the Recipient that they will process the Personal Data only for the specific purposes for which they were transferred and will not transfer them to a third party
   b. a determination by the Staff in Charge that the Recipient has implemented technical and organizational measures that will ensure adequate protection for the Personal Data that have been transferred.

ARTICLE 24: REQUESTS FROM AUTHORITIES

1. The ICRC's privilege of non-disclosure must be respected at all times, and any response to a request from authorities for access to Personal Data held by the ICRC must be coordinated in advance with the ICRC's Legal Division.

2. Data should be submitted to parties to an armed conflict, or to actors involved in other situations of violence, only after confirmation – through an 'impact assessment' analysis by the ICRC Staff in Charge – that handing over this information is unlikely to give rise to disproportionate risks to the Data Subject's personal safety or to that of his or her family or community.

ARTICLE 25: ACCESS FOR ADMINISTRATIVE OR GENEALOGICAL RESEARCH

1. The ICRC Staff in Charge may consider disclosing Personal Data to third parties searching for Data Subjects or to Data Subjects' families seeking access to the ICRC's archives for administrative reasons or for genealogical research; in both cases, however, the decision to disclose data is subject to the conditions mentioned in this chapter.

C. Brueser/ICRC

CHAPTER 5
IMPLEMENTATION

ARTICLE 26: EFFECTIVE IMPLEMENTATION

1. Effective implementation of these rules is crucial to ensure that Data Subjects are able to benefit from the protection afforded by them. Effective implementation is ensured by the work of the following entities, as well as by the ICRC Staff in Charge: the ICRC Data Protection Office and the ICRC Data Protection Commission.

2. It is the task of the ICRC Staff in Charge to make sure that these rules and the ICRC's data protection policies are implemented.

3. ICRC Departments at headquarters in Geneva and ICRC field structures are responsible for drawing up effective and suitable measures to guarantee that their activities comply with the principles and commitments laid down in these rules.

4. Allegations of non-compliance with these rules must be reported immediately to the ICRC Staff in Charge, who should investigate them without undue delay. If a complaint is found to have merit, appropriate measures should be taken to mitigate any risk of harm to the Data Subject.

5. Any breach of these rules that results in harm to Data Subjects must be referred to the Human Resources Department at ICRC headquarters and to field structures by the ICRC Data Protection Office. ICRC staff members involved in a serious breach may be subject to disciplinary measures.

ARTICLE 27: ICRC DATA PROTECTION OFFICE

1. A Data Subject who believes that his or her rights under these rules have been infringed may petition the ICRC Data Protection Office.

2. If it cannot find a solution, the ICRC Data Protection Office must refer the matter to the ICRC Data Protection Commission.

3. If any questions arise regarding compliance with the conditions for data Processing, the ICRC Data Protection Office must consult the ICRC field structure or, if at headquarters in Geneva, the Division concerned in order to obtain clarification or supplementary information that may clear up the matter. The ICRC Data Protection Office together with the ICRC field structure or Division concerned must also take any other steps necessary to ensure that these conditions have been met. The ICRC Data Protection Office must inform and advise the ICRC Staff in Charge of its obligations pursuant to these rules; it must also document these activities and the responses to them.

4. The ICRC Data Protection Office is also responsible for:
   a. monitoring the implementation of these rules with regard to data protection by design and by default
   b. monitoring whether Data Protection Impact Assessments are carried out by the ICRC Staff in Charge or a Processor, in accordance with these rules
   c. maintaining records of all categories of Processing activity within its responsibility
   d. approving the creation of or alterations to a database
   e. devising training modules
   f. broadening awareness of data protection issues among ICRC staff
   g. supervising implementation of these rules and ensuring respect for them.

5. When there is an urgent need to act in order to protect the rights and freedoms of Data Subjects, the ICRC Data Protection Office is entitled to adopt provisional measures with a specified period of validity.

6. The ICRC Data Protection Office does not receive any instructions for carrying out the tasks mentioned above or for providing advice. Data Protection Officers shall not be dismissed or penalized in any other way for performing their duties.

ARTICLE 28: ICRC DATA PROTECTION COMMISSION

1. The ICRC Data Protection Commission is responsible for interpreting these rules, and for rendering decisions about the implementation or breach of the rules.

2. When the ICRC Data Protection Office submits a case to it, or when a Data Subject petitions it, the ICRC Data Protection Commission has jurisdiction to examine all questions of fact and interpret the rules relevant to the matter and make binding decisions.

3. Advisory opinions from the ICRC Data Protection Commission shall be sought with regard to ICRC strategies and policies, the use of technologies new to the ICRC, and complex or large-scale Processing operations – when these have, or when there is a possibility of their having, an adverse impact on Data Subjects' rights.

C. Von Toggenburg/ICRC

CHAPTER 6

REVIEW AND UPDATE

ARTICLE 29: REVIEWING AND UPDATING THESE RULES

1. To ensure the ICRC's responsiveness to regulatory, social and technological developments in the area of data protection, these rules are to be reviewed by the ICRC Directorate and, subsequently, by the ICRC Assembly at least every three years.

2. To facilitate the periodic review, the Data Protection Office shall submit a yearly report to the ICRC Assembly. The report shall provide an appraisal of challenges encountered in applying these rules, legal and technological developments, and changes in attitudes and approaches to the Processing of Personal Data by States, and humanitarian and other non-State actors, that are relevant to ICRC operations.

3. Following the periodic review, the ICRC shall update these rules accordingly.

ANNEX

DEFINITIONS

Active Data means all Personal Data processed by the ICRC that is not Archived Data; **Active Database** means a database containing Active Data.

Archived Data means Personal Data contained in documents that have been transferred to the ICRC's Archives Division, which will manage and/or be responsible for such data; Archived Data ceases to be Active Data. Documents containing Archived Data constitute ICRC **Records**, and, as such, cannot be deleted or modified.

Consent means any freely given, specific and informed indication of his or her wishes by which a Data Subject signals agreement to the Processing of Personal Data relating to him or her.

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

Data Controller means the natural or legal person, which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

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

Data Transfer includes all acts that make Personal Data accessible to third parties outside the ICRC – on paper, via electronic means or the internet, or through other methods.

The ICRC Rules on Personal Data Protection apply to the Processing of Personal Data by automated means as well as to manual Processing, if the data are held or intended for holding in a filing system.

Genetic Data means Personal Data relating to the genetic or inherited characteristics of an individual that have been acquired through analysis of a biological sample from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or by analysis of any other genetic or inherited element that enables the acquisition of equivalent information.

Health Data means data related to the physical or mental condition of an individual that reveal information about the state of his or her health.

Personal Data relating to health includes in particular:

- data pertaining to the physical or mental condition of a Data Subject
- information about registration for health services
- a number or symbol assigned to an individual to uniquely identify the individual for health purposes
- information derived from testing or examining a body part or bodily substance, including Genetic Data and biological samples
- any information on a disease, disability, mental-health or psychosocial disorder, disease risk, medical history or clinical treatment, or information on the physiological or biomedical state of the Data Subject
- any information on a traumatic experience that had an adverse effect on the Data Subject's mental health or led to psychosocial disorders.

ICRC Controller means ICRC headquarters in Geneva, Switzerland, which, alone or jointly with others, determines the purposes for Processing Personal Data and the means of doing so. Such determination is based on the guidelines, policies, and decisions of the relevant Division and/or Region of the Operations Department, where applicable, in coordination with the ICRC Data Protection Office.

ICRC Data Protection Independent Control Commission or **ICRC Data Protection Commission** means the independent body that is responsible, and entrusted with the necessary authority, for carrying out the relevant tasks set out in the ICRC Rules on Personal Data Protection, and in particular for ensuring the existence of effective and enforceable Data Subject rights and of effective and independent means of redress.

ICRC Data Protection Office means the Unit that is responsible, and entrusted with the necessary authority, for carrying out the tasks set out in the ICRC Rules on Personal Data Protection. The ICRC Data Protection Office must not be confused with the ICRC Protection Data Unit.

ICRC Staff in Charge means the ICRC staff member in each ICRC field structure and headquarters Division who is entrusted by the ICRC Controller with the management of a particular area of activity within the ICRC's mandate. This includes protection coordinators, assistance coordinators, communication coordinators, cooperation coordinators, administration coordinators, and, where they are present, economic security coordinators, water and habitat coordinators, health coordinators, forensics coordinators, and ICRC management. At ICRC headquarters, ICRC Staff in Charge means the Heads of Division or staff members delegated by them to act as ICRC Staff in Charge.

Personal Data means any information relating to an identified or identifiable natural person. This may include an identifier such as a name or audiovisual materials, an identification number, location data or an online identifier; it may also mean information that is linked specifically to the physical, physiological, genetic, mental, economic, cultural or social identity of a Data Subject. The term also includes data identifying or capable of identifying human remains.

To determine whether a person is identifiable, all the means reasonably likely to be used – either by the controller or by any other person – to identify the individual directly or indirectly should be taken into account. To ascertain what means are reasonably likely to be used to identify the individual, all objective factors – such as the costs of identification and the amount of time required for it, given the technology available at the time of the Processing and technological developments – should be taken into account. Therefore, Personal Data does not include anonymous information, that is, information that 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 is no longer identifiable. The ICRC Rules on Personal Data Protection do not, therefore, cover the Processing of such anonymous information, including for statistical and research purposes.

Persons who use online services may be associated with online identifiers provided by their devices, applications, tools and protocols – such as Internet Protocol (IP) addresses or cookie identifiers – which constitute Personal Data. Such use of online services may leave traces that, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them.

Processing means any operation or set of operations – by automated and other means – that is performed upon Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmitting, disseminating or otherwise making available, aligning or combining, or deleting.

Processor means a person, public authority, agency or other body that processes Personal Data on behalf of the ICRC Controller.

Profiling means any automated Processing of Personal Data for creating or using a personal profile by evaluating various aspects of a natural person's life – in particular, analyses and predictions related to performance at work, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Recipient means a person, public authority, agency or other body – that is, someone or something other than the Data Subject, the Data Controller or the data Processor – to which the Personal Data is disclosed.

The ICRC helps people around the world affected by armed conflict and other violence, doing everything it can to protect their lives and dignity and to relieve their suffering, often with its Red Cross and Red Crescent partners. The organization also seeks to prevent hardship by promoting and strengthening humanitarian law and championing universal humanitarian principles.

People know they can count on the ICRC to carry out a range of life-saving activities in conflict zones and to work closely with the communities there to understand and meet their needs. The organization's experience and expertise enables it to respond quickly and effectively, without taking sides.

facebook.com/icrc
twitter.com/icrc
instagram.com/icrc

International Committee of the Red Cross
19 avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org

ICRC

4261/002 02.2020 300