Annex 4: THE ICRC RULES ON PERSONAL DATA PROTECTION

Contents:

INTRODUCTION

Background

Data protection rights legislation has been developing rapidly in recent years and further legislation in this regard is currently being developed.

As new technologies are developing 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 the private sphere of individuals 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 its 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) while abiding by internationally recognized standards for protecting Personal Data.

They apply solely to the Processing of Personal Data. Defined terms appear in capital letters throughout these rules and are defined in this annex.

Processing under a mandate

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.

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 Frame 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;

"Controller" means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the Processing of 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 Swiss Confederation – 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 characteristics of an individual that have been inherited or acquired, resulting from the analysis of a biological sample (BS) from the individual in question, in particular by chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;

"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 relevant ICRC Rules on Personal Data Protection. The ICRC Data Protection Office must not be confused with the ICRC Data Protection 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;

"Processing" means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"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;

"Technical and organisational security measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CHAPTER 1: BASIC PRINCIPLES

Article 1. Legitimate and fair Processing

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

2. The ICRC may process Personal Data only if there is a legitimate basis for doing so. 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
    e. Performance of a contract; and
    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 Subjects, such as children, the elderly, the mentally disabled or people who have been psychologically traumatized.

Article 2. Transparent Processing

1. Data Processing must always 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 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 should 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 purpose/s for which data are processed, and only processes them 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 should 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 inaccurate Personal Data are corrected or deleted without undue delay (taking into account the purposes for which they are processed).

Article 6. Retention, destruction, 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 erased or archived.

2. Personal Data should 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); or
    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.

CHAPTER 2: RIGHTS OF DATA SUBJECTS

Article 7. Information

1. The following minimum information about data Processing must be provided to Data Subjects when Personal Data are obtained or collected:

    a. whether the ICRC is the Data Controller;
    b. the basic elements of the ICRC's mandate;
    c. the purpose 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.

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 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 should be given an opportunity to verify their Personal Data, and should be given access to them except in the circumstances listed in paragraph 4, 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. 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 security or to that of his or her family or community.

4. 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.

5. 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 below.

6. 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.

7. It is legitimate for people to seek to reunite their families, to inquire 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 should be weighed against the confidentiality of Personal Data and the rights and interests of Data Subjects.

8. Access to Archived Data is subject to strict conditions and procedures.

Article 9. Correction

1. At the request of a Data Subject, mistakes or inaccuracies in his or her Personal Data may 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. Erasure

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

2. However, the right to erasure 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 erasure because of external pressure, and that erasing 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; or
   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, personal preferences, 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.

2. When it cannot settle an individual complaint itself, the ICRC Data Protection Office refers the matter to the ICRC Data Protection Commission. If a complaint is found to be justified, appropriate measures should be taken.

Article 14. Derogations

If the ICRC's humanitarian mandate 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 appropriate to these circumstances after consultation with the ICRC Data Protection Office and the director of the ICRC Department in charge.

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.

2. This requires that when the ICRC cooperates with another entity in Processing data, the responsibilities of all parties concerned should 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 it 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 Art. 17).

Article 16. Data protection by design and by default

1. While designing a database 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 connection 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 as to 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 activities within its remit.

Article 19. Cooperation with supervisory authorities

1. Any compliance with national data protection legislation and/or 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, should 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 without undue delay when the Data Breach puts them at particularly serious risk, unless:

    a. that would involve disproportionate effort, owing to logistical circum-stances 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 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; or
    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 should be processed in a manner that ensures an appropriate degree of security. 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 cybersecurity, the duty of discretion and the conduct of staff.

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

CHAPTER 4: DATA TRANSFERS

Article 22. Definition of Data Transfers

Data Transfers, particularly across national borders, are a routine occurrence during ICRC activities. The term ‘Data Transfer’ is to be broadly construed: it includes any act that makes Personal Data accessible, whether on paper, via electronic means or the internet, or any other method to entities outside the territory of Switzerland.

Article 23. Limitations on Data Transfers

1. Personal Data may be transferred only to the extent permitted by these rules.
2. Data Transfers are subject to strict conditions:

    a. Processing by the Recipient is restricted as much as possible to the specific purposes of ICRC Processing or permissible further Processing;
    b. 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;
    c. The transfer should not be incompatible with the reasonable expectations of the Data Subject; and

d. The transfer fulfils the conditions applicable under Article 24.1 and 24.2., below.

3. Depending on the sensitivity of the transfer and the risks it presents to individuals, additional protections may be necessary. A record of Data Transfers should be maintained. It may also be necessary to carry out a Data Protection Impact Assessment in connection with the data to be transferred.

Article 24. Transfers

2. Transfers may be legitimate when appropriate safeguards are adopted, such as:

a. ensuring that they are made to an adequate Recipient, that is, a Recipient who is subject to the data protection legislation of one of the countries listed on the website of the Swiss Federal Data Protection and Information
b. Commissioner;
c. using contractual clauses ensuring data security and appropriate levels of data protection.

3. Other permissible grounds for transferring data include:

a. the Consent of the Data Subject;
b. the vital interests of the Data Subjects or of other persons;
c. the public interest, based on the ICRC's mandate under IHL and/or the Statutes of the Movement;
d. the legitimate interests of the ICRC;
e. the fulfilment of a contract with the Data Subject;
f. the fulfilment of a Contract with a third party; or
g. the defence of legal claims.

3. Transfers within the Movement are permitted, provided they are based on important reasons linked to the public interest, the vital interests of the Data Subject or of another person, and/or the Data Subject's Consent.

4. In order to fully protect Data Subjects' Personal Data, the ICRC must ensure that its specific status is recognized, and all parties concerned must be made aware that the ICRC cannot be obliged to disclose any information acquired in the course of its activities. More specifically, the ICRC's privilege of nondisclosure must be respected. Any response to a request from authorities for access to Personal Data held by the ICRC should be coordinated in advance with the ICRC's Legal Division.

5. Appropriate measures should be used to safeguard the transmission or forwarding of Personal Data to third parties. The means of transmission, and the methods of security employed, should be consonant with the nature and sensitivity of Personal Data, the risks revealed by the Data Protection Impact Assessment and the urgency of humanitarian action.

CHAPTER 5: IMPLEMENTATION

Article 25. Effective implementation

1. Effective implementation of these rules is crucial to ensure that people 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 such implementation is provided.

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 should be immediately reported 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 should 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 26. ICRC Data Protection Office

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

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

8. 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.

9. The ICRC Data Protection Office is also responsible for:
   - monitoring the implementation of these rules with regard to data protection by design and by default;
   - monitoring whether Data Protection Impact Assessments are carried out by the ICRC Staff in Charge or a Processor, in accordance with these rules;
   - maintaining records of all categories of Processing activity within its responsibility;
   - approving the creation of or alterations to a database;
   - devising training modules; and
   - ensuring that these rules are regularly reviewed in light of developments in the regulatory sphere, and/or in response to the need to adapt them to changes in ICRC activities. If a significant amendment to these rules becomes necessary, the ICRC Data Protection Office should submit a proposal to that end to the ICRC Directorate for approval.

10. 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.

Article 27. ICRC Data Protection Commission

11. The ICRC Data Protection Commission is responsible for interpreting these rules.

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