Adopted by the ICRC Assembly: 28 August 2019

Policy on the Processing of Biometric Data by the ICRC

1. Purpose of this Policy

1.1. The purpose of this Policy on the Processing of Biometric Data by the ICRC ("the Policy") is to ensure that the processing of biometric data by the ICRC takes place in accordance with the principle of "do no harm", the humanitarian imperative, the ICRC protection mandate and the ICRC Rules on Personal Data Protection ("the Rules").[1] It also seeks to ensure that those Rules are applied in a manner that takes into account the specific features of biometric data and the opportunities and risks associated with their processing.

1.2. The application of data protection rules to humanitarian action is imperative to safeguard the rights and dignity of individuals, to support the implementation of the "do no harm" principle, and to enhance the accountability and transparency of organizations processing personal data. For the ICRC, the protection of personal data whose disclosure could put its beneficiaries at risk, or otherwise be used for purposes other than those for which it was collected, is an integral means of preserving its neutrality, impartiality, and independence, as well as the exclusively humanitarian nature of its work.

1.3. The ICRC recognises that the responsible deployment of new technologies including biometric identification techniques can enhance the capacity of its operations and the realisation of specific, mandate-based objectives.

1.4. Biometric data are categorised as sensitive personal data in a growing number of jurisdictions, and consequently their processing under those legal regimes is subject to specific legal restrictions, and is in some cases prohibited. While the ICRC processes personal data in accordance with its own Rules, status, mandate and privileges and immunities, those Rules require heightened protection of personal data whose disclosure could give rise to harm to individuals. These principles are underscored by the ICRC's Professional Standards for Protection Work, which require humanitarian actors to assess threats to persons providing them with information and take necessary measures to avoid negative consequences to those persons. It follows that if data is too sensitive and could result in harm to Data Subjects that cannot be mitigated then the data should not be collected in the first place. The ICRC and Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action also recognises that biometric data pose specific risks and challenges for humanitarian action.[2] The ICRC has therefore adopted this Policy in recognition of the acute concerns associated with the processing of biometric data. In particular, the Policy requires the ICRC to limit the use of biometric data to specific use cases and modalities, conduct Data Protection

[1] Available at: https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.
[2] *Handbook on Data Protection in Humanitarian Action*, Brussels Privacy Hub & ICRC, 2017 (see Chapter 8).

Impact Assessments in advance of any new project or programme involving biometric data, adopt a data protection by design and by default approach to all biometric systems, be transparent about its use of biometric data, and ensure the rights of Data Subjects are upheld whenever such data are processed.

1.5. Due to rapid technological change and evolving data protection norms in this area, the Policy also commits the ICRC to regularly review its implementation to ensure that the processing of biometric data does not inadvertently jeopardise the rights or safety of Data Subjects. This recognizes potential developments in the capability of particular biometric identification or analytical techniques and changing attitudes and approaches to the use of biometric data by States, humanitarian and other non-state actors. It also aims to ensure that any new privacy enhancing technologies that may be developed over time can be adopted, enabling increased use of biometrics use cases, if required.

1.6. This Policy sets out:

(i) the roles and responsibilities of the ICRC staff and programmes;
(ii) the Legal Basis for processing biometric data by the ICRC;
(iii) the specified purposes and use cases pursuant to those legal bases;
(iv) authorised biometric data types and processing techniques;
(v) data protection impact assessment and data protection by design and by default requirements;
(vi) conditions to be met for the engagement of third parties to collect or process biometric data on the ICRC's behalf;
(vii) conditions for and restrictions to data transfers, including requests for access to governments, law enforcement and judicial bodies; and
(viii) measures to ensure respect for Data Subjects' rights, including transparency requirements.

2. Scope of application

2.1. The Policy applies to all biometric data processed by ICRC staff and programmes in accordance with their official duties and activities, as well as to personal data processed by the ICRC for the purpose of creating a biometric 'template' or 'profile' regardless of format. As such it includes biological reference samples, images used for digital matching, and the 'converted' data created for the purposes of comparison.

2.2. The Policy also applies to National Society staff authorised to process biometric data on behalf of the ICRC by the Staff in Charge of a particular ICRC programme, as applicable.

2.3. Core elements of the Policy also apply to situations in which the ICRC may use biometric data processed by partners or service providers for the purposes of authenticating or verifying the identity of its beneficiaries, even if that data is not actually processed by the ICRC, pursuant to Article 13.

2.4. The Policy applies to the biometric data of ICRC staff, with the exception of biometric data that ICRC staff may be required to provide to States or other organisations for the purposes of enabling international travel, or to any biometric data that ICRC staff may volunteer or otherwise provide to external entities not acting under the instruction of the ICRC (for example, in using biometrics to protect their mobile devices or access the premises of other organisations).

3. Definitions

3.1. "Anonymization" means converting personal data into anonymised data so that it is no longer possible to identify the individuals to whom the data relates. Data is not anonymised if this process can be reversed, either by de-coding, or through techniques such as data matching, which enable re-identification.

3.2. "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.

3.3. "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.

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

3.5. "Data Protection Impact Assessment" means the exercise of identifying, evaluating and addressing the risks to Personal Data arising from a project, policy, programme or other initiative implemented by the ICRC.

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

3.7. "Personal Data" means any information relating to an identified or identifiable natural person. This may include an identifier such as a name or audio-visual 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.

3.8. "Pseudonymisation" means substituting personally identifiable information such as an individual's name with a unique identifier that is not connected to their 'real world' identity using techniques such as coding or hashing.

3.9. "Staff in Charge" means the ICRC staff member in each field structure or at the Headquarters who is entrusted with the management of a particular area of activity or programme within the ICRC mandate. The Staff in Charge includes programme coordinator and the ICRC management, or staff members delegated by them to act as the ICRC Staff in Charge.

4. Roles and responsibilities

4.1. The ICRC is the Controller of the biometric data and associated Personal Data it processes in accordance with the ICRC Rules on Personal Data Protection, as specified in this Policy, when it determines the purpose and means for which it may be used, including when such data may be shared with partners.

4.2. The ICRC Directorate is responsible for the approval of new cases pursuant to Article 6.4 and the periodic review of this Policy and the adoption of any changes pursuant to Article 21 of this Policy.

4.3. The ICRC Department Director in charge of the relevant programme/division is responsible for ensuring that operations and administration comply with this Policy, and that any new use cases or processing techniques are subject to a Data Protection Impact Assessment pursuant to Articles 6.4 and 7.3. They are also responsible for ensuring that all ICRC staff and partners involved in the collection and processing of biometric data are familiar with this Policy and appropriately trained as to their data protection obligations. These tasks may be delegated by the programme/division Director as appropriate.

4.4. The ICRC Data Protection Office (DPO) is responsible for the oversight of this Policy and:

(i) the provision of guidance, upon request or on its own initiative, regarding the processing and protection of biometric data;

(ii) monitoring the compilation and regular update by the Staff in Charge, pursuant to Article 4.6, of a register of the ICRC processing operations involving biometric data;

(iii) the approval of any further processing of biometric data and biometric processing modalities pursuant to Articles 6.3 and 7.3;

(iv) providing support and guidance to Data Protection Impact Assessments conducted in accordance with Article 10.3;

(v) assessing the adequacy of the data protection safeguards adopted by partners and service providers pursuant to articles 12 and 13;

(vi) considering requests for access to biometric data pursuant to articles 14 and 15;

(vii) responding to requests, objections and complaints from Data Subjects concerning the processing of their Personal Data referred to the DPO in accordance with Article 20; and

(i) facilitating the periodic review of the Policy pursuant to Article 21, and, in particular, preparing and presenting an annual report for the ICRC Assembly as set out in Article 21.2.

4.5. The ICRC's ICT Security staff is responsible for ensuring that biometric IT solutions adhere to the mandates in the ICRC Information Security Framework and the ICRC Information Handling Typology considering that biometric data is to be classified as "strictly confidential". It is also responsible for assessing the adequacy of the information security provisions implemented by partners and service providers pursuant to articles 12 and 13.

4.6. The Head of Delegation in the field operations bears overall responsibility for the processing of biometric data by the ICRC in a given country while the Director in charge of the relevant services at HQ bears responsibility for the processing of biometric data by the ICRC at HQ. Both are

responsible for the application of the Policy and must ensure that the following provisions are implemented (these tasks may be delegated as appropriate):

(i) the application of the data minimisation principle with respect to the collection and further processing of biometric data in accordance with Article 8;
(ii) the maintainance of a record of processing operations involving biometric data;
(iii) the maintainance of a record of any data transfers involving biometric data in accordance with Article 15.

4.7. The Staff in Charge of an ICRC programme using biometric data in a given country must ensure that the following provisions are implemented (these tasks may be delegated as appropriate):

(i) the application of the data minimisation principle with respect to the collection and further processing of biometric data in accordance with Article 8;
(ii) biometric data is only retained as long as it is needed for the purposes for which it was collected in accordance with Article 17;
(iii) Data Protection Impact Assessments are conducted in accordance with Articles 6 and 10 and sign them off;
(iv) Data Breaches involving biometric data are responded to in accordance with Article 16;
(v) Data Subjects are provided with information about the processing of their biometric data at the point of collection, or, if applicable, subsequently, in accordance with Article 18; and
(vi) requests, objections and complaints from Data Subjects concerning the processing of their Personal Data are responded to in accordance with Article 20.

5. Legitimate basis for the processing of biometric data by the ICRC

5.1. Pursuant to the ICRC's Rules on Personal Data Protection, the legitimate basis for the processing of biometric data for the specific purposes set out in Article 6 are:

(i) the "important grounds of public interest" in using biometric data linked to a mandate to identify individuals in order to provide specific humanitarian services requiring the identification of human remains and separated or missing persons affected by conflict, other situations of violence and other humanitarian emergencies;
(ii) the "legitimate interest of the ICRC" in using biometric data to:
   a. protect strictly confidential information and mission critical resources;
   b. to provide beneficiaries of humanitarian services with a token-based verification credential that can be used to verify their receipt of those services, where the token is held by the Data Subject and no database of biometric data is maintained by the ICRC.

6. Specified purposes of the processing of biometric data by the ICRC

6.1. Biometric data is processed by the ICRC for specific humanitarian purposes and may only be used for those purposes.

6.2. Following a comprehensive review of its biometric data processing operations, the following use cases have been approved by the ICRC for these specific humanitarian purposes:

(i) the inclusion of the fingerprints of the holder on travel documents issued by the ICRC to persons who have no valid identity papers, enabling them to return to their country of

origin or habitual residence or to go to a country which is willing to receive them, with processing of such data restricted to the use of ink to reproduce fingerprint images on the actual travel documents;[3]

(ii) the use of biometric identification systems to restrict access to strictly confidential information and/or mission critical resources such as servers and control rooms in ICRC premises, where the processing of such data is restricted to specific internal locations requiring a high level of security and those staff authorised to access them;[4]

(iii) the use of fingerprint data, facial scans and DNA to identify human remains recovered from disaster or conflict zones or in connection with other situations of violence;[5]

(iv) the use of digitised photographs for the purposes of tracing and clarifying the fate of separated or missing persons;

(v) the use of biometric data to ascertain the identity or fate of specific individuals in the course of investigations related to the abduction of, or attacks upon, ICRC staff members;

(vi) on a case-by-case basis, where it is has been determined that it is in the best interests of the persons concerned, the collection of biological reference samples for the purposes of DNA profiling to facilitate family reunification or determining the fate of a missing person where proof that two persons are actually related is required under national law or policy;[6]

(vii) the provision of beneficiaries of humanitarian services and assistance with a token-based verification credential such as a card that can be used to verify their receipt of those services, where the token is held on a support held by the Data Subject, and no data base of biometric data is held by the ICRC.

6.3. Beyond the purposes clearly authorised above, biometric data held by the ICRC may only be further processed for a compatible humanitarian purpose, without the need for an update of this Policy by the Directorate pursuant to Article 21, subject to the approval of the Data Protection Office. A request for further processing for compatible humanitarian purposes shall be submitted by the Staff in Charge to the Data Protection Office, and the request shall clearly set out how the further use is deemed to be compatible, based on the following compatibility criteria:

(i) the link between those purposes and the purposes of the intended further processing;

(ii) the situation in which the data were collected, including the reasonable expectations of the Data Subject as to their further use;

(iii) the nature of the Personal Data;

(iv) the consequences of the intended Further Processing for Data Subjects;

(v) appropriate safeguards; and

(vi) the extent to which such safeguards would protect the confidentiality of the Personal Data.

---

[3] Note that ICRC does not convert these images into machine-readable data or documents or retain them in a central database.

[4] ICRC delegations may not therefore use biometrics for routine premises control requiring the mandatory biometric enrolment of all ICRC staff.

[5] Note that these data are not retained by the ICRC in any central database, though the facial images of deceased persons may be compared with an ICRC database such as 'Trace the Face' for the purposes of matching them to a person reported missing.

[6] Note that ICRC's internal "Guidance on ICRC involvement in the use of DNA analysis to establish family relationships for the purpose of family reunification" considers this procedure as a 'last resort' and contains extensive data protection safeguards.

6.4. Further use cases, not deemed compatible with the purposes approved and listed above, may be approved by the ICRC Directorate upon revision and update of this Policy in accordance with the provisions set out in Article 21.

7. Authorised biometric data types and processing techniques

7.1. The ICRC may process fingerprints, facial images and biological reference samples collected for the purposes of creating a DNA profile for the specified purposes set out above according to the criteria set out below.

7.2. The ICRC may use the following techniques to process biometric data:

(i) fingerprinting using ink and biometric scanners for the purposes of identifying human remains;

(ii) fingerprinting using biometric scanners for the purposes of enrolling staff and beneficiaries into biometric verification systems;

(iii) facial recognition for the purposes of matching facial images;

(iv) the comparison of DNA profiles for the purposes of matching relatives.

7.3. Further physiological biometric data and processing techniques may be approved by the ICRC DPO on a case-by-case basis following the completion by the Staff in Charge of a Data Protection Impact Assessment pursuant to Article 10. This Policy will be updated to include newly authorised biometric data and processing techniques in accordance with the provisions set out in Article 21.

8. Adequacy, relevance and minimisation of biometric data

8.1. In accordance with the ICRC Rules on Personal Data Protection, data processed for a specified purpose must be relevant and not excessive in relation to the particular purposes. In accordance with this requirement, where the ICRC intends to process biometric data, it must first establish that the intended purpose and required outcome(s) of the processing could not be achieved without using biometric data.

8.2. In accordance with the principles of data adequacy, relevance and destruction of data that is no longer needed, the ICRC must ensure that biometric data and the additional personal data that is associated with it is processed to the minimum extent possible. In practice this means collecting only the data that is strictly necessary to achieve the intended purpose(s); deleting biometric data as soon it is no longer needed in accordance with Article 17, restricting access to the data in accordance with the 'need to know' principle and other safeguards outlined in Article 11, and not sharing biometric data unless such transfers fulfil the conditions set out in Articles 12 to 14.

9. Non-mandatory nature of biometric processing by the ICRC

9.1. Whilst certain humanitarian services provided by the ICRC in order to realise its mandate-based objectives may not be possible without the processing of biometric data (for example, DNA

matching of human remains), the ICRC will not make the provision of biometric data a mandatory condition of service provision.

10. Data Protection Impact Assessment for processing operations involving biometric data

10.1. For established use cases and processing techniques, a Data Protection Impact Assessment must be carried out by the relevant programme or Delegation prior to the establishment of any new project or programme involving biometric data. Where a DPIA addressing the data protection and information security risks has already been conducted for a similar project or programme and is deemed applicable to intended processing, a further DPIA is not required.

10.2. In conducting the Data Protection Impact Assessment, the ICRC must assess the risk that it, or any partners or service providers involved in the processing, may not be in a position to resist requests to access data from authorities. This assessment must be subject to regular review.

10.3. A Data Protection Impact Assessment must also be conducted by the ICRC prior to the organisation using biometric data collected by other humanitarian organisations to authenticate or verify the identity of recipients of the ICRC's humanitarian services in accordance with Article 13.

10.4. A Data Protection Impact Assessment must also be conducted prior to transferring biometric data to a government or authority for humanitarian purposes pursuant to Article 14.

10.5. A copy of any Data Protection Impact Assessment performed in respect of biometric data must be provided to the Data Protection Office.

10.6. For new processing techniques or use cases referred to in Articles 6.4 and 7.3, the Data Protection Office must be consulted prior to the start of the Data Protection Impact Assessment, and may give directions as to its focus and content, the mitigating measures to be taken, and means of implementation.

11. Data protection by design and default and security of biometric data processing

11.1. The ICRC must ensure that new systems, programs and projects processing biometric data are developed according to the data protection by design and default principle. This requires the implementation of high level data security features and technical and organisational measures that ensure the requirements of this policy are met by design and by default. Data protection by design and default also requires the adoption of the least intrusive and lowest risk processing modality pursuant to the considerations in Annex 1.

11.2. Legacy systems involving the processing of biometric data that were established before this Policy was adopted should be reviewed and enhanced pursuant to these requirements.

11.3. Having regard to the functional needs of the biometric system, the ICRC must develop or deploy the following security features:

(i) biometric data is protected by state of the art data security measures including the encryption of data at rest and in transit to minimise the risk of unauthorised access;
(ii) systems are designed to prevent the unauthorised disclosure of biometric data using technical means including the 'one way encoding' of biometric images and the use of proven algorithms for biometric template conversion and matching;
(iii) notwithstanding the need to maintain a link between these datasets, database instances are segregated, with biometric data records stored separately from the personal data with which they are associated; and
(iv) audit trails are established for the use of all biometric data processed by the ICRC.

11.4. When designing biometric systems and having regard to the functional needs of the biometric system, the ICRC must ensure that:
(i) a beneficiary-centric (or user-centric) approach to the ownership of the data is built in to the system architecture and associated policies, ensuring that the Data Subject is informed about the processing, can access their data, understand how it has been used, and make decisions about its continued processing;
(ii) the principle of data minimisation is effectively implemented with regard to the processing of personal data linked to a biometric profile, which is strictly limited to information that is necessary to meet the specified purpose; and
(iii) pseudonymisation techniques are applied to the processing of the personal data associated with the biometric data.

11.5. When implementing biometric systems, the ICRC must ensure that:

(i) in accordance with the ICRC's Professional Standards for Protection Work, Accountability to Affected Populations framework, Data Subjects and beneficiary communities are involved in the programmatic design and risk assessment and mitigation process;

(ii) access to biometric data by ICRC staff, partners and third-party service providers is restricted as far as possible and procedures to meet the requirements of Article 12 are in place;

(iii) standard operating procedures are followed to ensure that all personal data is accurate and up to date and that every reasonable precaution is taken to ensure that inaccurate data are corrected or deleted without undue delay; and

(iv) technical and organisational measures and oversight thereof prevents any further processing of biometric data for purposes other than the specified purpose for which it was collected.

12. Use of partners and service providers to process biometric data on the ICRC's behalf

12.1. Logistical, operational or technical constraints may require the ICRC to enlist the support of humanitarian partners, such as National Societies of the Red Cross and Red Crescent, or service providers, such as forensic laboratories providing DNA analysis, to achieve the objectives and pursue the activities specified in Articles 6 and 7. These arrangements must be subject to the following safeguards.

12.2. Third parties may only be enlisted to process biometric data upon instruction of the ICRC subject to all of the following conditions being met:

(i) the engagement of the third party is necessary for the effective implementation of the specified humanitarian purpose and service in question;

(ii) the third party is or agrees to be bound by data protection safeguards that meet the standard required by the ICRC Rules on Personal Data Protection and of this policy, and agrees not to process the data for any other purposes than those for which it is provided unless explicitly authorised to do so by the ICRC; and

(iii) the processing will not, in the assessment of the Staff in Charge, involve any risk to the life, safety, dignity, integrity of the Data Subject and/or the Data Subject's family, or of other people.

12.3. Where the intended processing of biometric data meets the above conditions, the following safeguards must be implemented prior to the processing taking place:

(i) in cases where the ICRC enlists the support of a partner to provide a specific humanitarian service, a data processing agreement setting out the basis, purpose of the processing and the restrictions to which it is subject is in place, and specific organisational and technical measures have been devised to minimise access to the biometric data and the period in which it is in their custody;

(ii) in cases where the ICRC engages the services of an external provider to process biometric data, a contract or written agreement binding the provider to solely act upon the

instructions of the ICRC and implement specific technical and organisational measures to protect the personal data against any unauthorised form of processing is in place;

(iii) the agreement with the processor recognises that the data remains under the control of the ICRC and is covered by the ICRC's status and the privileges and immunities it enjoys, and is bound to respect the privilege of non-disclosure and consult the ICRC Staff in Charge prior to acting on any response to a request from authorities for access to personal data processed under the instruction of the ICRC. It must be possible to implement effectively these guarantees;

(iv) the agreement with the processor contains provisions for immediate notification of the ICRC in respect of any data breach;

(v) the amount and type of Personal Data processed by the third party together with the biometric data is strictly limited to that which is necessary for the service provided and has been subject to a data minimisation review to this effect;

(vi) the processor agrees to delete the data as soon as the purpose for which it has been provided has been achieved and a procedure for verifying the deletion is in place; and

(vii) the processing is subject to a high level of security that prevents unauthorised access to the data.

12.4. The ICRC's DPO and ICT Security Services must be consulted for guidance on the assessment of the data protection framework of partners and the specific organisational and technical measures to be implemented by third parties to protect the biometric data processed on behalf of the ICRC.

13. Use of biometric data collected by third parties to verify the identity of recipients of humanitarian services provided by the ICRC

13.1. The ICRC recognises that where the Data Subject(s) has already provided their biometric data to another humanitarian organisation or is in possession of a card/device that is capable of verifying their identity by checking it against biometric data stored therein, it may be better from a data protection perspective to utilise this functionality in its own operations rather than processing additional biometric data. In this scenario, although the ICRC does not actually process any biometric data, it must ensure that the risks of utilising biometric data under the Data Subject or a third party's control are subject to a Data Protection Impact Assessment pursuant to Article 10 and that the transparency requirements in Article 15 are fulfilled.

13.2. In exceptional circumstances due to the security situation on the ground or the imposition of operating restrictions upon other humanitarian organisations, the ICRC may be requested to use or even take control of that organisation's biometric verification or identity management system for the purposes of continuity of aid provision to beneficiaries who would otherwise lose access to assistance or services. Where there is a humanitarian imperative for such as course of action, the ICRC may process the biometrics collected by another organisation on a temporary basis. A Data Protection Impact Assessment must then be conducted to assess the necessity, risks and implications of the processing and devise technical and organisational measures to bring the processing into line with the ICRC Rules on Personal Data Protection. The DPIA must be completed and recommendations as to how to bring the processing in line with the requirements of this Policy must be put forward to the Directorate for a decision on how to proceed within six months of the ICRC assuming control of the data.

14. Requests for access to biometric data by authorities

14.1. The ICRC is aware of the value of biometric data in locating and identifying persons of concern to States and security, law enforcement and judicial bodies and is conscious that these authorities also have a significant interest in obtaining such data from organisations operating in humanitarian emergencies. This interest can extend to using biometric data for purposes that, while in some cases entirely legitimate from the point of view of the authorities, may be incompatible with the neutrality, impartiality and independence of the ICRC, as well as the exclusively humanitarian nature of its work and the vital interest of the Data Subject. These purposes could include border and migration control, counter-terrorism activities and national security.

14.2. In order to safeguard the neutrality, impartiality and independence of the ICRC and the exclusively humanitarian nature of its work, the ICRC will not share or otherwise transfer biometric data to any government or authority, unless all of the following conditions are met:

(i) the transfer is in the vital interest of the data subject or of another person;

(ii) the transfer is necessary in order to enable an authority to fulfil an obligation of a humanitarian nature;

(iii) the Data Subject is informed that the data transfer is envisaged and does not object (unless the data subjects are unaccounted for and the purpose of sharing is indeed to identify the whereabouts of the data subject or identify human remains);

(iv) a Data Protection Impact Assessment (DPIA) is carried out prior to the data sharing, and the DPIA does not highlight risks for the data subjects or other persons which take primacy over the perceived benefits of the sharing; and

(v) The recipient commits in writing to only use the transferred data for the specified humanitarian purpose.

14.3. Where the Staff in Charge is in receipt of a request from authorities and believes that there may be difficulties for the ICRC to comply with the requirements above, the ICRC DPO must be promptly informed, and, if necessary the ICRC DPO must escalate the matter to the Directorate for decision.

15. Transfer of biometric data to third parties

15.1. Biometric data may only be transferred to third parties in accordance with Articles 12 to 14.

15.2. Other requests by third parties for access to biometric data for exclusively humanitarian purposes may be considered on a case-by-case basis. Such requests must be referred to the ICRC DPO, which, if necessary, may escalate the matter for a decision by the Directorate.

15.3. All transfers of biometric data from the ICRC to third parties must be subject to dedicated technical and organisational measures providing a high level of security that prevents unauthorised access to the data.

15.4. In all cases of transfer of data to external entities, the Staff in Charge must ensure that a documentary record of transfers is maintained, which includes the following:

(i) Name of the recipient/organisation;
(ii) Date of transfer;
(iii) Description of the categories of Personal Data that have been transferred;
(iv) Purpose of the transfer; and
(v) Limitations on the use of data agreed upon by the recipient.

16. Data Breaches

16.1. In case of a Data Breach affecting the biometric data stored on the premises of ICRC in Geneva, or by a partner or service provider acting under its instruction, the ICRC will notify the ICRC Delegation which input the data that it has been breached, as well as the Delegations covering the territory where the data subjects are likely to be, and the ICRC Data Protection Office.

16.2. In case of a local Data Breach affecting biometric data stored on the premises of an ICRC delegation, or by a partner or service provider acting under its instruction, the Staff in Charge must be informed as soon as the breach is identified. The Staff in Charge must communicate the breach to the ICRC HQ and the ICRC Data Protection Office.

16.3. If specific actions are required to mitigate risks arising from the Data Breach, including, if appropriate, notification to the affected beneficiaries, these will be taken in accordance with established ICRC procedures and with the assistance of the ICRC Data Protection Office and the ICT Security Office.

16.4. The persons affected must be notified of a Data Breach without undue delay when the Data Breach puts them at particularly serious risk, unless:

(i) 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 similar measure whereby the Data Subjects are informed in an equally effective manner;
(ii) it would adversely affect a matter of substantial public interest, such as the viability of the ICRC's operations or security of staff; or
(iii) approaching the Data Subjects, because of the security conditions, could endanger them or cause them severe distress.

17. Retention of biometric data by the ICRC

17.1. All biometric data should be subject to a retention period explicitly linked to the specific purpose for which it was collected. Biometric data may be retained by the ICRC for only as long as it is needed for this specific purpose.

17.2. If at the end of the retention period it is established that the biometric data are no longer required then the data must be deleted. If at the end of the retention period it is established that the

biometric data are still required by the ICRC for the specified humanitarian purpose, or for a compatible humanitarian purpose, the retention period may be renewed or extended.

17.3. No archiving of biometric data by the ICRC is permitted, unless specifically determined in an Accord where ICRC acts as a neutral intermediary and Data Subjects have consented to this.

18. Transparency of biometric data processing by the ICRC

18.1. In the interest of transparency and accountability this policy is published on the ICRC's website.

18.2. The processing of biometric data must be rendered transparent to Data Subjects by the ICRC through the systematic provision of programme-specific information to affected populations clarifying how and why such data will be utilized.

18.3. Where biometric data is collected directly from the Data Subject, whether by the ICRC or a partner acting upon its instruction, those persons must be provided with the following information, either at the point of collection, or, taking into account the literacy of the affected population, in advance through prior outreach to community representatives or community information campaigns:

(i) the identity and contact details of the Data Controller;
(ii) the grounds for and purpose of the processing of the biometric data;
(iii) the identity of any external entities to whom the data will be transferred and the purpose of such transfers;
(iv) the fact that the Data Subjects have rights in respect of the processing of their biometric data and are entitled to more information about these rights upon request.

18.4. Further information regarding the data protection framework for the use of biometrics by the programme must be made available to Data Subjects or community representatives upon request. This should include, in addition to the information specified above:

(i) any risks inherent in the processing of biometric data that are specifically related to the vulnerability of the affected population and the technical and organisational measures that have implemented to safeguard the data and mitigate any identified risks;
(ii) the details of any third party service providers involved in the programme as processors of biometric data;
(iii) the limitations on transfers to authorities pursuant to Article 14;
(iv) the rights of the Data Subjects pursuant to Article 20;
(v) the contact details of the ICRC Data Protection Office and the ICRC Independent Data Protection Control Commission.

18.5. Where biometric data is not collected directly from the Data Subject but provided to or otherwise obtained by the ICRC, the processing must be rendered transparent by the publication of a programme-specific data protection policy by the responsible Delegation or Division. Where appropriate, taking into account security conditions in the field, logistical constraints, the capacity of the Data Subjects, and the urgency of the Processing, the minimum information included in Article 18.3 should be disseminated through outreach to community representatives and information campaigns addressing the affected population.

18.6. All information and communication concerning the processing of biometric data must be accessible and easy to understand, and provided in clear and plain language.

19. Rights of the Data Subject

19.1. All individuals whose Personal Data is processed by the ICRC enjoy the rights set out in the ICRC Rules on Personal Data Protection. The ICRC is committed to ensuring that these rights are fully respected when biometric data is processed and confirms that Data Subjects:

(i) have the right to request access to Personal Data concerning them, including biometric data processed by the ICRC;[7]

(ii) have the right to rectify/correct Personal Data concerning them, including biometric data processed by the ICRC, for example in respect to erroneously processed facial images or DNA samples;

(iii) have the right to request the deletion of Personal Data concerning them, including biometric data held by the ICRC. In principle, this data may be deleted in the following cases: the biometric data are no longer needed to achieve the primary purpose or any other compatible purpose; the Data Subject objects to the processing of their biometric data; or the processing of biometric data does not comply with this Policy or the ICRC Rules on Personal Data Protection.

20. Procedures for handling requests, objections and complaints concerning biometric data processing

20.1. The Staff in Charge of an ICRC program in which biometric data are processed is responsible for responding to any requests from Data Subjects concerning access to their Personal Data, the correction or deletion of their Personal Data, and objections to or complaints regarding the processing of their Personal Data. If the request or complaint cannot be resolved to the satisfaction of the Data Subject it should be escalated to the ICRC Data Protection Office in a timely manner.

20.2. In the case of objections to the provision of biometric data by the Data Subject the ICRC must provide the humanitarian services to the Data Subject without processing their biometric data.

20.3. In the case of requests for access to biometric data, the Staff in Charge is responsible for conducting an identity check to ensure that the person requesting the data or making the complaint is the Data Subject or, in the case of parents or legal guardians, duly entitled to make such a request on their behalf. Records of such requests must be maintained and the responses and any related correspondence kept on file in case the Data Subject makes further complaints or appeals.

[7] The right of access does not cover access to the Personal Data of other individuals, though family members or legal guardians of Data Subjects may request data on their behalf where the individual lacks the age of majority or capacity to do so.

20.4. The Staff in Charge should aim to respond to such requests within two weeks and not later than four weeks. If it is not possible to comply with the request within this time frame the Staff in Charge should inform the Data Subject of the delay and notify the ICRC Data Protection Office.

20.5. Where the Staff in Charge is unable to comply with Data Subject requests or remedy their complaints, either fully or in part, on the basis of one or more of the above grounds, they must explain this to the Data Subject and inform them of the possibility to have this decision reviewed, through the ICRC Data Protection Office and the Independent Data Protection Control Commission.

21. Review and updates to this Policy

21.1. In order for the ICRC to remain responsive to social, technological and legal changes in this field, this policy is to be reviewed by the ICRC Directorate at least every three years.

21.2. The periodic review shall be facilitated by a yearly report by the DPO to the ICRC Assembly, providing an overview of the ICRC biometric data processing operations that involve an assessment as to their ongoing necessity and proportionality. The report shall also provide an appraisal of challenges experienced in the application of this policy, legal and technological developments and changing attitudes and approaches to the use of biometric data by States, humanitarian and other non-state actors that are relevant to the ICRC operations.

21.3. The periodic review shall also take into account any new use cases and processing modalities with respect to biometric data pursuant to Articles 6.4 and 7.3.

21.4. Following the periodic review the ICRC shall update this Policy accordingly.

Annex 1: Factors to be considered in assessing risk and adopting a data protection by design and default approach to the processing of biometric data

NB

1. Without a legitimate/lawful basis for processing, the use of biometrics remains illegitimate irrespective of risk profile.
2. Level of risk for indicative purposes only. "Lower risk" does not mean no risk. Like-for-like comparisons cannot be made across different factors/variables.
3. An asterisk (*) denotes that a particular option is in any case prohibited by the Policy.

Factor	Lower risk	Higher risk	Highest risk
Type of biometric	Not widely used as a biometric (e.g. palm vein) and not currently possible to derive additional information from image	Widely used as a biometric and possible to compare with other datasets (e.g fingerprints)	Widely used as a biometric and easy to compare with other datasets (e.g. facial images), or to derive additional information from (e.g. iris)
Cultural acceptability	Use of biometric accepted by beneficiary population	Use of biometric raises concerns among beneficiary population	* Use of biometric unacceptable to beneficiary population
Immutability of biometrics		Individuals enrolled in a biometric system seek to evade identification capabilities and in order to do inflict self-harm (e.g. by mutilating fingerprints)	Individuals enrolled in a biometric system cannot evade identification capabilities (e.g. DNA or Iris)
Purpose & functionality	Authentication (1:1)	Identification/de-duplication (1:many)	
Biometric enrolment	Leverage token-based or smart phone capability to avoid collection/processing	Leverage humanitarian partner authentication app to avoid collection/processing	ICRC collects and processes biometrics
Storage medium	Biometrics stored in an individual token/card held by data subject (and not the ICRC)	Biometrics stored in central database held by ICRC or service provider	* Biometrics stored in a blockchain system

Factor	Lower risk	Higher risk	Highest risk
Data Hosting Model	On ICRC premises	Fully "jurisdictional" cloud under ICRC control	* Cloud service where technical and organisational measures are insufficient to guarantee full jurisdictional control
Retention of biometric image	Images deleted after template conversion	Images stored in local database (offline)	Images stored in central database (online)
Template conversion process	Biometric cryptosystem (with keys required for authentication or identification)	Non-invertible transformation (one way encoding) of biometric images	Biohasing (or salting) of biometric data (more easily invertible/ reversible)
Separation of biometric data	Biometrics stored separately and linked to minimal programmatic enrolment data	Biometrics stored separately and linked to identity management system	Biometrics integrated into population database/identity management system
Access and re-use	Access strictly limited (need to know) to programme staff	Provision for use across multiple programmes or services	* Permanent records created linked to beneficiary registration and available to all database users
Retention	Biometric data deleted after use in specific programme	Biometric data retained for use in additional programmes or services	* Biometric data retained on a permanent basis
Controller/ processor	Data under full control of ICRC and subject to P&Is	Data processed jointly with or by third parties which risks data not being protected by ICRC's P&Is	Data processed by third parties and not under ICRC's "jurisdictional" control
System architecture	"Zero knowledge" (whereby ICRC cannot see or extract biometrics)	Technical measures restricting access to biometric records and preventing bulk download	Biometric data can be viewed and copied/downloaded
Encryption	Data encrypted at rest, in transit and in process	Data encrypted in transit but not at rest, or vice versa	* Data not encrypted at rest or in transit