International Commission of Jurists
Data Protection Policy

Last modification	Authorized by	Scheduled for review
September 2024 (v.1)	Executive Committee	October 2027

1. Introduction

1.1 The International Commission of Jurists (ICJ) recognizes the importance of protecting the confidentiality, integrity, and availability of the data it handles. This Data Protection Policy establishes principles and guidelines for the collection, storage, processing, and disposal of data to ensure compliance with relevant data protection laws and regulations.

1.2 To advance its mission of promoting human rights and ensuring access to justice for all, ICJ may collect and utilize personal information from commissioners, donors, employees, consultants, interns, suppliers, beneficiaries, partners, visitors, and other relevant stakeholders.

1.3 The processing of personal data touches all areas of ICJ's operational and administrative activities. This policy is based on an initial data inventory and risk assessment that examined the types of data ICJ holds and how it is collected, processed, stored, and disposed. This policy, as the data inventory and risk assessment, is intended to be a living document.

2. Definitions

The terms used in this policy are defined below.

Data Controller: An individual or organization that determines how and why personal data is processed. ICJ and its officers are Data Controllers.

ICJ Data Processor or Users: An individual or organization that processes data on behalf of the data controller. Any member of ICJ's staff can be a data user.

Data Subject: An individual who can be identified, directly or indirectly, by reference to Personal Data.

ICJ Data Focal Points: ICJ staff, consultants and or officers, selected by the ICJ Senior Management Team (SMT),who ensure the ICJ Data Protection policy and standard procedures are followed and made known to internal and external stakeholders.

Data Transfer: Any act that makes personal data accessible, whether on paper, via electronic means or the internet, or any other method to any third party not linked in a way or another to ICJ.

Data Breach: Any type of security breach 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.

Personal Data: 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.

Processing: 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 erasing.

Sensitive Personal Data: Specific categories of personal data that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, health-related data, or information regarding a person's sex life or sexual orientation.

3. Scope

3.1 This Policy applies to all ICJ employees, contractors, third-party vendors, and subcontractors who have access to the ICJ's data, regardless of the format or medium in which it is stored and irrespective of the location and office type. This policy also applies to the ICJ Executive Committe, Commissioners and the Secretary General.

3.2 This policy encompasses globally recognized data protection principles while complementing existing national laws. In instances where there is a conflict between this policy and national laws, national laws will take precedence. However, adherence to this policy is required even in jurisdictions lacking equivalent national legislation.

4. Principles

Below are the principles governing this policy:

4.1. Lawfulness, Fairness, and Transparency

i. The ICJ processes personal data lawfully, fairly, and transparently, ensuring that individuals are aware of the purposes for which their data is being collected and processed. ICJ will only collect and process personal data for legitimate interests tied to its mission or out of regulatory and contractual necessity.

ii. The ICJ processes personal data transparently ensuring that communications with data subjects is clear and accessible. ICJ will provide sufficient information regarding the processing of personal data at the point of collection in clear and plain language.

4.2 Purpose Limitation

i. Personal data will only be collected for necessary and legitimate purposes directly related to ICJ's mission and will not be further processed in ways incompatible with those purposes.

ii. Sensitive personal data will only be collected when required by law or otherwise necessary to further ICJ's mission, and upon prior written consent of the data subject.

4.3 Accuracy

The ICJ will ensure that Personal Data is accurate and, where necessary, kept up to date. Reasonable steps will be taken to rectify or erase inaccurate data without delay.

4.4. Storage Limitation

The ICJ will retain Personal Data only for as long as necessary to fulfil the purposes for which it was collected or as required by applicable laws and regulations.

4.5. Security

The ICJ will implement appropriate technical and organizational measures to ensure the security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

4.4. Accountability

The ICJ will be accountable for complying with this policy and will regularly review and assess its data protection practices ensuring ongoing compliance.

4.5. Integrity and Confidentiality

The ICJ personal data users must treat personal data in a confidential manner. They must ensure that Personal Data is securely stored with suitable organisational and technical measures to prevent unauthorised or illegal processing.

5. Rights of Data Subjects

ICJ respects the rights conferred to data subjects including:

5.1 Information Rights

Data subjects must be informed about their rights regarding their personal data processing and transfer to third parties before any processing or transfer occurs

5.2 Access Rights

i. Data subjects may request access to their personal data held by ICJ through a written request using the designated form annexed to this policy entitled Data Subject Access Form.
ii. Access to personal data is not granted automatically. The ICJ personal data controllers must first consider all circumstances surrounding the request for access and allow access only after verification.

5.3 Correction Rights

Data subjects may request corrections to inaccurate or incomplete personal data, with changes made once identity is verified.

5.4 Deletion Rights

Data subjects can request deletion of personal data in writing if continued processing lacks a legal basis or if it no longer serves its original purpose.

5.5 Personal Data Portability Rights

Data subjects have the right to request a copy of their personal data in a format that is easy to use and transfer. If ICJ processes an individual's personal data based upon their consent or to fulfill a contract, and if that data is handled using automated methods, the individual can request in writing that ICJ provide the data directly or transfer it to another party.

5.6 Objection Rights

Data subjects may object to processing on legitimate grounds unless outweighed by ICJ's contractual obligations, interests or legal obligations.

5.7 Processing Restriction Rights

Data subjects have the right to request the restriction of their personal data processing under certain circumstances. This means that while ICJ may continue to store their personal data, it will not process it further. Data subjects can exercise this right when:

i. The accuracy of the personal data is contested by the data subject, for a period enabling ICJ to verify its accuracy.
ii. The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction instead.
iii. ICJ no longer needs the personal data for processing purposes, but it is required by the data subject for the establishment, exercise, or defense of legal claims.
iv. The data subject has objected to processing based on legitimate interests pending verification of whether ICJ's legitimate grounds override those of the data subject.

5.8 Rights related to Automated Processing

ICJ recognizes that individuals have the right not to be subject to decisions based solely on automated processing, including profiling for recruitment or other purposes. ICJ does not engage in automated decision-making or processing but should this change, it will inform data subjects about its practices and provide the opportunity to contest any resulting decisions, and it will implement appropriate safeguards.

6. Responsibilities

6.1 Management

i. ICJ's SMT is responsible for establishing and promoting a culture of data protection compliance within the organization, allocating resources for implementing necessary measures, and overseeing the effectiveness of data protection efforts.
ii. Designation of Data Protection Focal Points
SMT will designate one Data Protection Focal Point for data related to human resources and one for data related to programme implementation. The SMT may designate additional Data Protection Focal Points for other types of data if needed.

6.2 Employees, contractors, and third-party vendors

All employees, contractors, and third-party vendors are responsible for complying with this policy, handling data in accordance with its principles and procedures, and reporting any suspected breaches or violations to the appropriate authorities.

7. Procedures

7.1 Data Protection by Design and by Default

The principles of data processing and the rights of data subjects outlined in this policy must be thoroughly considered and incorporated during the design and application of all ICJ systems and processes.

7.2 Data Collection and Processing

Personal data will only be collected and processed with the explicit consent of the data subject or as otherwise permitted by law. Data Subjects will be informed of the purposes for which their data is being collected and processed.

7.3. Consent Management

ICJ will maintain a comprehensive consent management approach that emphasizes clarity, specificity, and the rights of data subjects.

7.3.1 Clear and Informed Consent
ICJ will ensure that consent is obtained explicitly from data subjects before processing their personal data. This consent must be informed, meaning that individuals are provided with clear information about the specific type of data being collected, the purposes of processing, and any potential risks involved.

7.3.2 Voluntary Consent

Consent must be given voluntarily without any coercion or undue pressure and data subjects will be informed about their right to withdraw consent. Additional safeguards and accommodations will be put in place for vulnerable individuals to ensure informed consent.

7.3.2 Documentation and record keeping

Consent must be obtained in writing to the extent possible, unless otherwise permitted by law. ICJ will develop standardized templates for obtaining consent that include all necessary information in clear and plain language. All data users and Data Protection Focal Points will ensure that proof of informed consent is maintained and stored in accordance with this policy.

7.4 Data Security

i. The ICJ has implemented technical measures to protect electronically and non-electronically stored personal data from unauthorized access, disclosure, alteration, or destruction. The ICJ personal data users are committed to securely storing personal data and electronic equipment containing personal data in compliance with ICJ's security protocols and procedures.

ii. Additional technical and organizational measures will be adopted as necessary to protect personal data in all forms against unauthorized access, disclosure, alteration, or destruction. These measures may include encryption, limiting access or adding additional access controls, and regular security assessments.

7.5 Data Retention and Disposal

7.5.1 *Personal data in general*

i. Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected or as required by law. When personal data is no longer needed, it will be securely disposed of in accordance with established procedures.
ii. Personal data should preferably be stored on secure systems rather than personal devices. If personal data is kept on personal devices, strong passwords should be used. When using external tools not provided by the ICJ, users must ensure appropriate protective measures are in place before processing personal data and document these measures for auditing purposes.
iii. When personal data is stored physically or printed from electronic formats, it must be kept in a secure location inaccessible to unauthorized individuals (e.g. a locked drawer or filing cabinet).
iv. Documents and printouts containing personal data should not be left in accessible areas (e.g. on a printer) and must be securely shredded and disposed of when no longer needed.
v. Documents containing personal data may be kept for up to 10 years if required to fulfil regulatory and contractual obligations. All records should be securely destroyed or anonymized when retention is no longer necessary and or as long as required by law.

vi. ICJ will conduct data protection impact assessments (DPIAs) if processing activities are likely to result in a high risk to the rights and freedoms of individuals to determine additional safeguards needed.

7.5.2 *Personal data handled by Human Resources department*

i. All job applicants will receive an automatic response acknowledging their application and informing about the way their data is handled.
ii. Upon completion of the recruitment process, unsuccessful applications must be deleted or properly destroyed, unless explicit consent to retain the application has been provided by the applicant.
iii. Recruitment documents that include personal data must be viewed by people (e.g. recruitment officers, concerned line manager and service administrative).
iv. Sensitive questions are handled only for needs related to the position of work (e.g. conviction, debt, illness, etc.)
v. Criminal records are restricted only based on legal authority demands or donor's requirement.
vi. References from previous employers are obtained with the written consent of the job candidate and should focus on past performance and job behaviour, avoiding the collection of Personal and sensitive data.
vii. Access to the main Human Resources personal file is restricted to the HR department, the employee, their direct manager, and the manager's supervisor.
viii. Duplicate employment records can only be created with limited information if the employee is aware and a note in the main file indicates the duplicate's location.
ix. After an employee departs or separates from ICJ, their personal file must be retained until the expiration of the certification right, which is 10 years. Afterward, the personal data must be securely destroyed or appropriately anonymized.

7.5.2 *Personal and sensitive data held for implementing funded projects and activities*

ICJ is dedicated to balancing its regulatory obligations with a strong commitment to safeguarding the rights of vulnerable populations, including victims of abuse. ICJ recognizes that data collection can significantly impact certain individuals, and therefore, will adhere to widely accepted human rights-centered approaches while implementing programmes and activities.

i. Clear informed consent must be obtained from subgrantees, participants, consultants, donors and other stakeholders prior to the collection of personal and sensitive personal data in circumstances including but not limited to:
   - Event/activity registration forms (for virtual and in-person events);
   - Post-event or other surveys, Key Informant Interviews (KIIs), other personal data collection for monitoring and evaluation purposes;
   - While collecting personal data from partners as part of the partner due diligence process;
   - While documenting human rights abuses and collecting other sensitive personal data to advocate on behalf of vulnerable individuals;

- Prior to emailing or mailing newsletters or other solicitations to distribution lists. These must include clear opt-out/unsubscribe instructions.

ii. If written consent cannot be obtained from a stakeholder, a record of the person's clear and unambiguous indication of agreement should be documented. Translation and reasonable accommodations must be provided to ensure stakeholders have access to the information needed to provide informed consent and understand their rights. ICJ is dedicated to balancing its regulatory obligations with a strong commitment to safeguarding the rights of vulnerable populations, including victims of abuse.

iii. Participants lists, database and other project documents containing personal data should be processed and stored to the minimum extent needed to fulfil donor and regulatory compliance requirements and should only be shared if required. If transfer is required, participant lists and other documents containing personal data must be anonymized prior to sharing with a donor, auditor or any authorized third party. Records documenting the consent procedures followed, including forms provided must be stored in case of audit or other regulatory inspection.

7.6 Data Breach Response

i. Any incident involving personal data, including its accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access during transmission, storage, or processing, must be promptly reported to the incident response team using the annexed Personal Data Breach Reporting Form. This form should be sent by email to the Secretary General, Director of Administration and Finance, and HR Manager.

ii. The incident response team will assess the situation, contain the breach, mitigate its effects, and notify affected parties and regulatory authorities as required by law within 72 hours.

7.7. Training and Awareness

Regular training and awareness programs will be provided to staff to ensure understanding of how this policy applies to their work and their related rights and responsibilities.

8. International Data Transfers

The International Commission of Jurists (ICJ) shall ensure that any transfer of personal data outside of Switzerland or the European Union (EU) is conducted in accordance with applicable data protection laws.

1. Personal data will not be transferred to a third country or international organization unless:
    - The receiving country provides an adequate level of data protection.
    - Appropriate safeguards are implemented, such as Standard Contractual Clauses (SCCs) ensuring that the data subjects' rights are upheld.

- Explicit consent has been obtained from the data subject after informing them of the risks associated with the transfer.

2. ICJ will maintain documentation of all international data transfers, including the legal basis for each transfer and any safeguards applied.

9. Review and Update

This policy will be reviewed and updated as necessary to ensure ongoing compliance with changes in applicable laws, regulations, and organizational requirements.

10. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with applicable laws and regulations.

11. Contact Information

For questions or concerns regarding this policy or ICJ's data protection practices, please contact the ICJ Director of Administration and Finance.

Annex 1

Personal Data Access Request Form

I. Personal Information			
Title		First Name	
Middle Name		Last Name	
Email Address		Telephone	
Address			

II. Data Subject Category I. Please specify the category of the Data Subject:			
☐ **ICJ Staff**	☐IJC-Consultant	☐ICJ Intern	☐ICJ Contractor
☐**ICJ Donor Org.**	☐Provider	☐Applicant	☐Beneficiary
Other: Please specify:			

III. Type of Request	
☐**Information Access**	☐Information Correction
☐**Information Deletion**	☐Data Transfer
☐**Data Breach**	☐Non-Compliance
☐ **Other: Please specify**	

IV. Data Access or Breach Report
Please provide detailed information (including relevant dates) regarding the data you are requesting for access, correction, or deletion, or report its breach as well as any additional details that could assist us in locating the relevant personal data and verifying your identity.
- - - - - -

V. Declaration
By signing and submitting this form, you confirm that you are the data subject named in the ICJ Subject Access Request Form. ICJ cannot process requests for your personal data submitted by another individual.

Full Name: ----------

Date: ---------- Place: ----------

Signature: ----------

Annex 2

Personal Data Breach Reporting Form

I. Incident Information			
Date of Breach		Time of Breach	
Date of Report		Reported By	

II. Contact Information			
Reporter Name		Position	
Department		Email	
Region		Phone Number	

III. Description of the Breach	
Type of Breach	
☐ Accidental Destruction	☐ Unlawful Destruction
☐ Loss	☐ Alternation
☐ Unauthorised disclosure	☐ Unauthorised Access
Other: (Please Specify)	
Description of the Incident: *(Provide a (Provide a detailed description of the incident, including how the breach was discovered, and any initial actions taken.)*	
Location of Breach: *(Physical location, system, or platform where the breach occurred.)*	

IV. Data Affected	
Please Specify Below the categories of Personal Data involved	
☐ Names	☐ Addresses
☐ **Email Addresses**	☐ Phone Numbers
☐ **Financial Information**	☐ Health Data
Other (Please Specify)	
No of Data Subjects Affected:	

V. Actions Taken	
Immediate Actions Taken:	

(Describe the immediate steps taken to mitigate the breach.)	- -
Further Actions Planned: *(Outline any additional **steps planned to address** the breach and prevent future incidents.)*	- - -

VI. Notifications
Have the Data Subjects Been Notified? ☐ Yes ☐ No
Have Relevant **Authorities Been Notified**? ☐ Yes ☐ No
Details of the Notifications: ***(Provide details of notifications, including the date, method of notification, and any responses received.)*** - -
VII. Additional Information: **I.**
- - -
Declaration: **By submitting this form, I confirm that the information provided is accurate and complete to the best of my knowledge.**

Full Name: ---------- Position: ----------

Date: ----------Signature: ----------