



Inter-Parliamentary Union

For democracy. For everyone.

145th IPU Assembly

Kigali, Rwanda
11-15 October 2022



145th IPU ASSEMBLY
2022 | Kigali, Rwanda

IPU personal data protection policy and procedures

*Endorsed by the IPU Governing Council at its 210th session
(Kigali, 15 October 2022)*

DEFINITIONS

Consent: Any freely given informed indication of an agreement by a Data Subject to the processing of their Personal Data, which may be given by a written or oral statement or by a clear affirmative action.

Data Controller: The IPU staff member who has the authority to oversee the management of, and to determine the purposes for, the processing of Personal Data will be considered the Data Controller.

Data Processing: Any operation or set of operations that is performed on Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying. “processed” means having undertaken the act of processing.

Data Processor: Any IPU staff member or a natural or legal person, agency, public authority including an implementing Partner or Third Party that is engaged in processing Personal Data on behalf of the Data Controller.

Data Subject: A natural person that can be identified, directly or indirectly, in particular by reference to Personal Data. Examples of potential Data Subjects may include IPU staff members or members of the IPU governing bodies, parliamentarians, suppliers, or any individuals whose Personal Data is included in information collected from any of the foregoing.

Data Transfer: Any act that makes Personal Data accessible, whether on paper, via electronic means or the internet or any other method, to a Third Party. To “transfer” Personal Data means undertaking a Data Transfer of such Personal Data.

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

Information Owner: The person accountable for specific information, which for the purposes of this Policy are the Division Directors or Managers, who should be considered Information Owners of all information generated by or entrusted to their respective divisions. Division Directors may delegate their responsibilities as Information Owners to individual(s) within their Divisions, as they deem appropriate.

IPU Secretariat: The IPU Secretariat comprises the totality of the staff of the Organization under the direction of the Secretary General of the IPU.

IPU Personnel: All IPU staff members and other personnel engaged under other types of contracts, including interns, secondees, consultants and external collaborators.

Personal Data: Any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

#IPU145

Sensitive Personal Data: Personal Data which form part of the core area of private life, such as racial or ethnic origin, political affiliations or opinions, religious or philosophical beliefs, trade-union membership, health status (including medical, biological or biometric data), financial or family/relationship situation (including marital status, sexual orientation or preference or sex life and dependents) of a Data Subject. Sensitive data also include some employment records of IPU employees, such as those relating to their performance and conduct. The political affiliation of parliamentarians is a matter of public record and does not fall within the scope of the definition of Sensitive Personal Data for the purposes of this policy.

Supplier: A person, firm, company or organization that provides works, goods or non-consultant services against a contract.

Third Party: Any natural or legal person, public authority, agency or anybody other than the Data Subject, the Data Processor and the IPU Secretariat (as the Data Controller) and the persons under the direct authority of the Data Processor and the Data Controller. Examples of Third Parties are Member Parliaments, other national governments, international governmental or non-governmental organizations, and private sector entities and individuals.

I INTRODUCTION

1. In carrying out its programmes and operations, the IPU Secretariat collects, stores and processes Personal Data on individuals interacting with the IPU, including parliamentarians, staff members and other individuals engaging with the Organization. The IPU is committed to respecting the dignity and privacy of these individuals, while balancing such rights with the IPU's ability to carry out its mandate.

2. The IPU, in light of its mandates and purposes, promotes universal respect for human rights and fundamental freedoms including the right to privacy, and recognizes the importance of data protection policies, strategies and international standards that ensure the respect of those rights and freedoms. The purpose of this Policy is to define key principles in Personal Data Processing, outline the roles and responsibilities of the IPU Secretariat, its personnel and where applicable Third Parties. Personal Data protection laws and policies are intended to help protect an individual's rights to privacy while seeking to ensure that legitimate business and governance activities can be conducted within certain parameters.

II. SCOPE

3. This Data Protection Policy sets out the IPU's approach to data privacy protection. It outlines the processes followed by the IPU Secretariat to ensure that it can carry out its mandate while abiding by internationally recognized standards for protecting Personal Data.

4. This Policy applies to all IPU Personnel and, where applicable, Third Parties who receive, store and/or process any Personal Data (as defined above) and relate to all Personal Data received, stored and/or processed by the IPU Secretariat.

III. PRINCIPLES FOR PERSONAL DATA PROTECTION

5. The IPU Secretariat shall respect and apply the following principles when processing Personal Data:

A. Fair and Legitimate Processing

6. Personal Data shall be processed in a fair and transparent manner and only if there is a legitimate basis for doing so. Legitimate bases include:

- In the best interest of the Data Subject or another person;
- To ensure the safety and/or security of individuals;
- To enable the IPU Secretariat to carry out its mandate;
- Performance of a contract;
- Compliance with a legal obligation;
- Defence of legal claims.

7. The IPU Secretariat shall take particular care in processing Sensitive Personal Data. Sensitive Personal Data should only be processed where Data Subjects have given their explicit Consent except:

- as is necessary for the purposes of carrying out the obligations and specific rights of the IPU Secretariat under the Staff Regulations and Rules; or
- where processing is carried out in the course of the IPU Secretariat's legitimate interests on the condition that the processing relates solely to IPU Personnel or to persons who have regular contact with the IPU Secretariat in connection with its purposes, and that the Sensitive Personal Data is not disclosed to a Third Party without the Consent of the Data Subjects.

B. Limitation to a Purpose

8. Personal Data may be processed only for one or more specific and legitimate purposes and may not be further processed in a manner incompatible with such purpose(s). The IPU Secretariat 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. However, further processing is not permissible if the risks for the Data Subject outweigh the benefits of further processing.

C. Data Minimization

9. The processing of Personal Data shall be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, Personal Data that is being processed should be adequate and relevant to the identified purpose and should not exceed that purpose.

D. Accuracy

10. Personal Data shall be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed. Data Subjects should be made aware of the importance of providing accurate and complete information, including updating such information as applicable. Every reasonable precaution and effort will be taken to ensure that inaccurate Personal Data is corrected or deleted without undue delay (taking into account the purpose(s) for which it is processed, as well as the principles of data minimization and storage limitation).

E. Storage Limitation

11. Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose(s) for which the Personal Data is processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, statistical or historical research purposes.

F. Maintaining Security and Confidentiality

12. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

IV. RIGHTS OF DATA SUBJECTS

A. Right to Information and Access

13. Any person will be entitled to request information about their Personal Data. A Data Subject will be entitled to receive the following information from the IPU Secretariat:

- Confirmation as to whether or not Personal Data related to him or her has been, is being or is expected to be processed.
- Information on the Personal Data being processed, the purpose(s) for processing such data and any third parties to whom such data has been, is being, or is expected to be transferred and the envisaged period for which the Personal Data will be stored by these third parties.
- The information provided to the Data Subject in response to his/her request must be concise, transparent, intelligible and in an easily accessible form and in clear and plain language.

14. The IPU Secretariat will make information publicly available regarding the rights of Data Subjects under this Policy to access, correct, transfer and/or delete their Personal Data, including the means by which such a request can be made. In the event of such a request from a Data Subject, Information Owners within the IPU Secretariat will cooperate to compile the relevant information in a reasonable timeframe to be determined and agreed in coordination with the Data Subject.

15. The right of Data Subjects to access information does not apply or may be limited when important public interest requires that access be denied. These interests may include:

- Upholding confidentiality, such as that of whistle-blowers;
- Ensuring the viability of programmes and work-plans being carried out under the IPU's mandate;
- Preserving the confidentiality of IPU Personnel's views or line of reasoning, which, if breached, might jeopardize the IPU's operations and/or disclose the Personal Data of IPU Personnel;
- Preventing retaliation;
- Maintaining the privileges and immunities granted to the IPU;
- Defence of legal claims and compliance with legal obligations;
- Ensuring the integrity of audit, investigation or judicial processes; and
- The rights and freedoms of others that override the data-protection interests of the Data Subject.

16. The IPU Secretariat may also limit Data Subjects' right to access information if the Data Subjects' requests are manifestly excessive.

B. Right to Correction and Deletion

17. A Data Subject may request the correction or deletion of Personal Data that is inaccurate, incomplete, unnecessary or excessive, and the IPU Secretariat should correct or delete the Personal Data, as applicable, without undue delay. However, data may be retained in its original form if it pertains to historical records or other auditable information.

C. Right to Portability

18. A Data Subject may at any time request a copy of their Personal Data (in an easily accessible format) and/or request to have their Personal Data transmitted from the IPU Secretariat to another data controller.

D. Right to Objection

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

20. An objection of this kind will be accepted if the fundamental rights and freedoms of the Data Subject in question outweigh the IPU's legitimate interests, or the public interest, in processing the Personal Data. If such an objection is accepted, the IPU Secretariat should no longer process the Personal Data concerned. If there is a dispute with respect to an objection, the Information Owner shall be consulted and the final determination will be made by the Secretary General.

V. PROTECTION OF PERSONAL DATA PROCEDURES

A. Collecting Data from Data Subjects

21. When collecting Personal Data directly from a Data Subject, the IPU Secretariat will inform the Data Subject of the following:

- The specific purpose(s) for which the Personal Data or categories of Personal Data will be processed;
- Whether such Personal Data is intended to be transferred to a Third Party (including being made public);
- The importance of the Data Subject providing accurate and complete information, including updating such information as applicable; and
- The existence of this Policy and the means by which the Data Subject may request information or exercise their rights as provided herein.

22. Where possible, Data Subjects will be asked to acknowledge that they have received the above information and that by providing their Personal Data, they consent to the collection for the purpose articulated and the potential transfer, if applicable.

B. Suppliers

23. Where the collection and processing of Personal Data is one of the responsibilities of a Supplier, the IPU Secretariat will endeavour to ensure that the Supplier undertakes and respects the same or comparable standards and basic principles of Personal Data protection as contained in this Policy.

C. Confidentiality and Security of Personal Data

24. The IPU classifies Personal Data as confidential information. In particular, the IPU Secretariat ensures that Sensitive Personal Data is appropriately handled so as to preserve its confidentiality.

25. The IPU Secretariat's data security measures are designed and implemented to protect Personal Data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, or the unauthorized disclosure of, or access to, Personal Data. The IPU Secretariat maintains computer and information technology (IT) security that facilitate compliance with this Policy.

D. Ensuring Accuracy of Personal Data

26. IPU Personnel must ensure that the IPU Secretariat have their up-to-date personal information, as requested by the Director of Support Services. IPU Personnel must provide notice of any changes as soon as possible to ensure accuracy of personal records at all times.

27. The IPU Secretariat will update Personal Data records when necessary and periodically verify them. Personal Data held on its systems shall be deleted when it becomes known that such Personal Data is inaccurate, unnecessary or excessive. Where feasible and appropriate, confirmation from the Data Subject as to any correction should be obtained.

28. When Personal Data is corrected or deleted in the IPU Secretariat's systems as a result of having been inaccurate, unnecessary or excessive, any Third Parties to whom the relevant Personal Data was transferred should be contacted to the extent relevant and appropriate taking into account factors such as the original purpose of the transfer, whether the purpose is continuing and whether such notification would continue to be in compliance with the principles contained in this Policy.

E. Notification of a Data Breach

29. IPU Personnel are required to notify the Information Owner and the Director of Communication as soon as possible upon becoming aware of a Personal Data Breach or suspected breach and to properly record the breach. If Sensitive Personal Data has been or may have been compromised (e.g. unauthorized or unintended loss, modification, access or distribution), then this will be immediately reported.

30. If a Personal Data Breach is likely to result in personal injury or harm to a Data Subject, the Information Owner will use their best efforts to communicate the Personal Data Breach to the Data Subject and take mitigating measures as appropriate without undue delay, unless:

- doing so would involve disproportionate effort, owing to logistical circumstances or security conditions or the number of cases involved. In such cases, the Information Owner will consider whether it would be appropriate to issue a public statement or similar measure whereby the Data Subjects are informed in a manner that is reasonably expected to be effective;
- doing so would result in a breach of a legal obligation;
- doing so would jeopardize the IPU's privileges and immunities;
- it is necessary not to in order to defend legal claims; or
- approaching the Data Subjects, because of the security or political conditions, could endanger them or cause them severe distress.

F. Retention

31. Personal Data shall be retained only for as long as is necessary for the stated purpose(s) for which it was collected and processed without prejudice to the retention of records to be permanently or temporarily preserved for their administrative, fiscal, legal, scientific, historical or informational value.

VI. DATA PROTECTION BY THIRD PARTIES

A. Contractual Basis

32. If the IPU Secretariat cooperates with a Third Party in processing Personal Data, the responsibilities of both parties will be defined and set out in a contract between the IPU Secretariat and such other entity so as to allow the IPU Secretariat to ensure that confidentiality is maintained, to specify the specific purpose(s) and legitimate basis for the processing of Personal Data and to ensure continuing compliance with this Policy.

33. The Third Party shall not subcontract the Personal Data Processing to or engage another party without prior written authorization of the IPU. Any further addition or replacement of subcontractor by the Third Party shall be done under the same conditions.

34. Irrespective of any obligations set forth in an agreement, the IPU Secretariat will verify, prior to transferring Personal Data to a Data Processor or engaging a Data Processor in the processing of Personal Data, that the processing of Personal Data by the Data Processor satisfies the principles in this Policy.

VII. DATA TRANSFER

A. Limitations on Data Transfers

35. The IPU Secretariat may transfer Personal Data to Third Parties on the condition that the Third Party affords a level of data protection the same or comparable to the standards set out in this Policy, and Data Subjects have been made aware that their Personal Data may be transferred. In particular, and without limitation to the foregoing, Data Transfers are subject to the following conditions:

- The Data Transfer must be based on one or more legitimate bases;
- The Data Transfer must be for one or more specific and legitimate purpose(s);
- Processing by the Third Party must be restricted as much as possible to the specific purpose(s);
- The amount and type of Personal Data to be transferred is strictly limited to the Third Party's need to know for the specified purposes intended;
- The Data Transfer should not be incompatible with the reasonable expectations of the Data Subject; and
- The Data Subject's rights are respected and the recipient has at least adequate data protection and disclosure measures or guarantees and respects the confidentiality of the data that are disclosed by the IPU, maintaining an appropriate level of data security;
- The Data Transfer fulfils the applicable conditions set out in the Section on Safeguards below.

36. In carrying out its mandated activities, the IPU Secretariat may give restricted Personal Data access to its Members through the IPU Directory. Members will endeavour to ensure that they comply with the general principles of this policy and have safeguards in place for protection and security of such Personal Data entrusted to them by the IPU.

B. Transfer of Data to Member Parliaments and National Law Enforcement Agencies and courts

37. In appropriate circumstances and without prejudice to the IPU's privileges and immunities, the IPU Secretariat may transfer Personal Data to a Member Parliament or to a national law enforcement agency or a national court. Such transfers may be on the IPU's own initiative or upon request by the Member Parliament or national enforcement agency or court (which may be binding or non-binding on the IPU Secretariat). The transfer may concern persons subject to an investigation for an allegedly committed crime, human rights violation or in relation to the victim(s) of or witness(es) to a crime including leaders of NGOs who could potentially be qualified as "victims" or "witnesses". Such transfers which are not made on the IPU's own initiative would require authorization from the Secretary General, acting on recommendation of the Information Owner.

38. In addition to the general conditions for transferring Personal Data to third parties, the IPU may only cooperate with such requests and transfer Personal Data to a Member Parliament, national law enforcement agency or national court if the following conditions are met:

- (i) Transfer is necessary for the purpose of the detection, prevention, investigation or prosecution of a serious criminal offence relating to the safety and security of an individual or the public;
- (ii) The requestor is competent in relation to the detection, prevention, investigation or prosecution of the offence in question;
- (iii) The transfer will substantially assist the requestor in the pursuit of these purposes and the Personal Data cannot otherwise be obtained from other sources;
- (iv) The transfer does not disproportionately interfere with a Data Subject's or another person of concern's right to privacy or other human rights;
- (v) In the case of data in relation to victims and witnesses, their Consent to transfer has been obtained;
- (vi) Prior to the transfer of the Personal Data to the requestor, advice from the Data Protection Officer in consultation with the Legal Officer and Director of the division concerned needs to be sought.

C. Safeguards

39. In an effort to ensure that the principles set out above are adhered to, appropriate safeguards should be adopted, such as:

- The IPU Secretariat shall endeavour to ensure the implementation of appropriate organizational, administrative, physical and technical safeguards and procedures in order to protect the security of Personal Data processed by the IPU, including against or from unauthorized or accidental access, damage, loss or other risks presented by Personal Data Processing (Data Breaches).
- Events of suspected or actual Data Breaches shall be notified to the Data Subject as soon as practicable. The severity of such events shall be assessed, and appropriate measures, aimed at protecting affected Data Subjects, including mitigating or resolving possible adverse impacts, shall be taken without undue delay in accordance with internal procedures.
- Having regard to available technology, safeguards and procedures shall be reasonable and appropriate to the risks presented by the nature and processing of Personal Data and its level of sensitivity.

40. Unless there are satisfactory reasons not to do so, prior to transferring Personal Data to a third party, the Data Controller should seek to sign a Data Transfer agreement, or as appropriate, incorporate data protection clauses within broader agreements, particularly where transfers of Personal Data are likely to be large, repeated or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time.

41. Data Transfer agreements should, inter alia:

- (i) address the purpose(s) for Data Transfer, the specific data elements to be transferred, as well as data protection and data security measures to be put in place;
- (ii) require the third party to make sure that its data protection and data security measures are in compliance with this Policy; and
- (iii) stipulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer conducted under the agreement.

42. The Data Controller and the IPU Legal Officer shall review and authorize all Data Transfer agreements.

43. While every effort will be made to ensure the above safeguards are adhered to in the case of any transfer of Personal Data, other permissible grounds for transferring Personal Data include:

- The fulfilment of the objectives and mandates of the IPU
- The Consent of the Data Subject;
- The vital or best interests of the Data Subjects or other persons;
- The public interest, based on the IPU's mandate;
- To ensure the safety and/or security of individuals;
- The fulfilment of a contract between the IPU Secretariat and the Data Subject; or
- Defence of legal claims or compliance with legal obligations.

44. The IPU may receive Personal Data from third parties (Inbound Data):

- In cases where the IPU engages with third parties to collect Personal Data on the IPU's behalf, such third parties shall afford an appropriate level of security and protection for Personal Data in light of the principles of this Policy when collecting Personal Data;
- In cases where the IPU receives Personal Data from third parties that are not acting on behalf of the IPU, the IPU should take reasonable and proportionate steps to ensure that such Personal Data has been lawfully collected.

VIII. TRANSPARENCY

45. Insofar as the specified purposes for which Personal Data is processed are not frustrated, the IPU shall process Personal Data in a transparent manner, as appropriate and whenever possible, by providing Data Subjects with information about the processing of their Personal Data subject to conditions laid out in this policy, including whether Personal Data may be transferred to third parties, as well as information on how to request access, verification, rectification and/or deletion of their Personal Data.

46. Where such requests are manifestly abusive, fraudulent or too onerous to comply with given existing resources, the IPU shall decline to fulfil such requests.

IX. ACCOUNTABILITY

47. In order to ensure accountability for the processing of Personal Data and adequate implementation of this Policy, the Data Controller shall be responsible for establishing and overseeing the processing of Personal Data under his or her area of responsibility. He or she therefore also bears the main responsibility for compliance with the Policy.

48. The Secretary General may put in place more procedures, standards, guidelines and training, as well as an appropriate governance structure to ensure oversight of the processing of Personal Data, and redress mechanisms to handle requests and complaints from Data Subjects.

49. The IPU shall appoint personnel who shall be responsible for the implementation and control of IT security measures and procedures.

50. The IPU Secretariat and Member Parliaments will take all the possible measures and endeavour to ensure that the principles under this policy are respected while working with classified information and sensitive Personal Data entrusted or originating from the IPU to its Member Parliaments and will be responsible for keeping such information confidential. Failure to comply may be subject to disciplinary, or where applicable legal, actions and/or corrective measures.

X. PRIVILEGES AND IMMUNITIES

51. The adherence to and implementation of this Policy by the IPU is without prejudice to the privileges and immunities of the IPU. In particular, the processing of Personal Data by or on behalf of the IPU shall under no circumstances be deemed to constitute:

- (i) the acceptance of the applicability of any laws or regulations at the national, regional or international level, or
- (ii) the acceptance of the jurisdiction and the powers of courts or agencies or any other authorities, with respect of the processing activities undertaken by or on behalf of the IPU.