ITU Data Protection and Privacy Policy

I Purpose, rationale, scope and implementation

ITU considers data protection and privacy important and is committed to respecting privacy and protecting Personal Data. With this in mind, it endorsed the Personal Data Protection and Privacy Principles adopted by the United Nations High-Level Committee on Management on 11 October 2018.

The purpose of this Policy is to ensure that Personal Data is processed by ITU in line with those United Nations Personal Data Protection and Privacy Principles.

In carrying out its mandate, ITU processes Personal Data of various individuals, such as ITU staff and their family members, consultants, holders of Special Service Agreements, other members of ITU personnel, retirees, delegates, meeting participants, visitors, vendors and beneficiaries of assistance. ITU is responsible for providing transparency and establishing necessary safeguards to ensure protection of Personal Data.

This Policy covers ITU's processing of Personal Data of all Data Subjects. It is not applicable to the Personal Data of deceased persons or to non-Personal Data, including anonymized data, that cannot lead to the identification of an individual. Examples of Personal Data include a person's name, e-mail address, photograph and location data, the advertising identifier of a person's phone, Internet Protocol (IP) address and cookie ID.

The ITU Legal Affairs Unit (JUR) will provide advice to facilitate the implementation of this Policy. Any requests for guidance should be addressed to JUR, which is also responsible for leading the internal ITU Data Protection and Privacy Taskforce in the development of a detailed Guide on how to implement this Policy, including overall guidance on a number of issues raised herein, such as templates, clarifications on the designation of Internal Data Controllers and addressing requests from Data Subjects. Once identified, Internal Data Controllers will receive appropriate training on how to conduct Personal Data Mappings and Data Protection and Privacy Assessments. The Guide, which will be regularly updated, will also take into account relevant provisions of Recommendation ITU-T X.1058, which contains a code of practice for personally identifiable information protection.

II Terminology

The following definitions are applicable for the purposes of this Policy:

Consent

Consent is any freely given, specific and informed indication of an agreement by the Data Subject to the processing of their Personal Data.

Data Controller

The natural or legal person who, alone or jointly with others, has decision-making authority over the processing of specific Personal Data or sets of Personal Data.

Data Processing

Any operation or set of operations which is performed on Personal Data, irrespective of the technology and processes used, including by automated means, such as collecting, registering, recording, structuring, storing, adapting, cleaning, filing, retrieving, using, analysing, disclosing, transferring, sharing, providing access to, making available, erasing and destroying.

Data Processor

The natural or legal person who processes Personal Data under the supervision or direction or on behalf of the Data Controller.

Data Protection and Privacy Assessment

An assessment of the impact, including potential risks, harms and benefits, of the processing of Personal Data and identification of appropriate mitigation measures.

Data Subject

Any identified or identifiable natural person whose Personal Data is subject to processing. Such a person can be directly or indirectly identified by any means likely to be used, such as by using other available data and reasonably available expertise, skills, time and other resources.

Internal Data Controller

The designated ITU staff member who, alone or jointly with others, has decision-making authority within ITU over the processing of specific Personal Data or sets of Personal Data.

Personal Data

Information, in any form, that relates to an identified or identifiable natural person.

Personal Data Breach

A breach of security that leads to the accidental or illegitimate destruction, loss, alteration, disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Personal Data Mapping

A review of Personal Data processing activities in a written form that includes, at a minimum, the types of Personal Data processed, categories of Data Subjects, purposes and means of the processing, legal basis of the processing, systems where the processing takes place, applicable data security measures and information on any data transfers. A Personal Data Mapping shall also identify the Data Controller, which, in most cases, will be ITU, the Internal Data Controllers within ITU and any potential Data Processors.

Privacy Notice

A document that provides information to Data Subjects about the processing of their Personal Data by ITU in a clear and easily understandable manner. A Privacy Notice specifies, at a minimum, what Personal Data is collected and for what purpose, who has access to them, the rights of the Data Subjects and how those rights can be exercised.

Sensitive Personal Data

Personal Data that: (i) relates to racial or ethnic origin, political, religious or other opinions, beliefs or affiliations, migration status, trade union membership, genetic or biometric data uniquely identifying natural persons, health, gender, sex and sexual orientation; and (ii) any other Personal Data that the Internal Data Controller may designate as sensitive in a specific context. Sensitive Personal Data require the application of additional safeguards for their processing, such as the conducting of a Data Protection and Privacy Assessment or application of enhanced technical data security measures.

III Principles

1	FAIR AND LEGITIMATE PROCESSING	ITU shall process Personal Data in a fair manner, in accordance with its mandate and governing instruments and on the basis of any of the following: (i) the consent of the Data Subject; (ii) the vital interests or best interests of the Data Subject or another natural person; (iii) the ITU mandate, governing instruments and related resolutions; (iv) the discharge of ITU's functions in accordance with the ITU Staff Regulations and Staff Rules, ITU Financial Regulations and Financial Rules or any other internal mandatory policies, regulations and rules; (v) the performance or conclusion of a contract with the Data Subject; (vi) the conducting of investigations or for the establishment, exercise or defence of legal claims, or administration of justice; or (vii) an overriding legitimate interest of ITU.
2	PURPOSE SPECIFICATION	ITU shall process Personal Data for specified purposes, consistent with the ITU mandate and while taking into account the balancing of relevant rights, freedoms and interests of individuals. Personal Data shall not be processed in ways that are incompatible with such purposes.
3	PROPORTIONALITY AND NECESSITY	The processing of Personal Data shall be relevant, limited, adequate and not excessive to what is necessary in relation to the specified purposes of Personal Data processing.
4	RETENTION	Personal Data shall only be retained for the length of time necessary for the specified purposes to be fulfilled.
5	ACCURACY	Personal Data shall be accurate and, where necessary, up to date to fulfill the specified purposes.
6	CONFIDENTIALITY	Personal Data shall be processed with due regard to confidentiality. Confidentiality includes determining clear internal access controls to Personal Data or sets of Personal Data, which should be on a need-to-know basis.
7	SECURITY	Appropriate and adequate organizational, administrative, physical and technical safeguards and procedures shall be implemented to protect the security of Personal Data, including against unauthorized or accidental access, damage, destruction or loss. Examples of such safeguards include encryption and pseudonymization.
8	TRANSPARENCY	Processing of Personal Data shall be carried out transparently vis-à-vis the Data Subjects, including, for example, by providing information on the processing of their Personal Data and on how to request access to or verification, rectification and/or deletion of that Personal Data, provided that the specified purpose for which the Personal Data is processed is not frustrated. Privacy Notices should accompany all instances of Personal Data processing conducted by ITU.
9	TRANSFERS	In carrying out its mandated activities, ITU may transfer Personal Data to a third party, provided that, under the circumstances, ITU satisfies itself that the third party affords appropriate protection for the Personal Data. To ensure such appropriate protection, ITU shall only transfer Personal Data to a third party after having concluded a written agreement with that party.
10	ACCOUNTABILITY	ITU shall have adequate policies and mechanisms in place to adhere to these principles.

IV Data Subject rights and complaints

Data Subject rights

Data Subjects whose Personal Data are processed by ITU have the following rights:

1. **Right to access and verification**: the right to access and verify their Personal Data.
2. **Right to rectification**: the right to have their Personal Data rectified or completed if the data is inaccurate or incomplete.
3. **Right to information**: the right to be informed about the processing of their Personal Data, including the types of their Personal Data being processed and for what purpose, the legal basis for processing of the data, their rights and how to exercise them, and the sharing of their Personal Data with third parties, as appropriate.
4. **Right to deletion**: the right to have their Personal Data deleted when the data is no longer necessary for the purpose for which it was collected or when there is no legal basis for the processing of the data.
5. **Right to object**: the right to object to the processing of their Personal Data.

Exercising of rights and filing of complaints

Data Subjects may request to exercise their rights or file complaints in relation to the processing of their Personal Data by ITU by submitting a request to the Internal Data Controller, who shall verify the Data Subject's identity and assess the request or complaint before replying to it.

Should the Data Subject not be satisfied with the response of the Internal Data Controller, they may submit a request for review to the Secretary-General. The Secretary-General's response to the review request shall be considered final, without prejudice to any recourse that the Data Subject, e.g. ITU staff member, may have and with due regard to ITU's privileges and immunities.

A request or complaint may be rejected by ITU if it is manifestly unfounded, fraudulent or abusive or in view of reasons of public interest, safety and security, historical/statistical/scientific purposes, the discharge of ITU's mandate and functions or ITU's internal, contractual or confidentiality obligations.

V Data protection and privacy by design and by default

This Policy, including the relevant data protection and privacy organizational and technical safeguards, must be considered prior to the commencement of use of systems, platforms, software and procedures that involve the processing of Personal Data and during the design, use, deployment and maintenance thereof until the end of the use of the Personal Data.

The default settings of such ITU systems, platforms, software and procedures that involve the processing of Personal Data shall be set so as to ensure compliance with this Policy throughout the data processing lifecycle through, for example, the adoption of organizational, technical and physical safeguards.

VI Personal Data Mapping and Data Protection and Privacy Assessment

Internal Data Controllers are responsible for conducting Personal Data Mappings for the Personal Data or sets of Personal Data over which they have decision-making authority and for keeping them up to date.

Data Protection and Privacy Assessments are to be conducted by the Internal Data Controller when the Personal Data processing activities are likely to involve significant risks and impact on the Data Subjects, such as when processing involves Sensitive Personal Data or large amounts of Personal Data, or when processing involves the use of emerging technologies, e.g. artificial intelligence.

Data Protection and Privacy Assessments assess the impact, including potential risks, harms and benefits, of the processing of Personal Data and identify appropriate mitigation measures.

VII Personal Data Breach management

Any actual or suspected Personal Data Breach must be reported to the Internal Data Controller and the ICT Security Division of the Information Services Department. The ICT Security Division will coordinate the response to the Personal Data Breach, in consultation with the Internal Data Controller and JUR. The response will include the implementation of mitigation measures and the introduction of adjustments to data security protocols, as needed. The Internal Data Controller shall assess, in coordination with JUR, whether there is a need to notify Data Subjects of the Personal Data Breach.

A record of all confirmed Personal Data Breaches and how they were managed shall be kept by the Internal Data Controllers and ICT Security Division.