United Nations ST/SGB/2024/1

Secretariat

13 March 2024

Secretary-General's bulletin

Data protection and privacy policy for the Secretariat of the United Nations

The Secretary-General, inspired by the Organization's long-time efforts in applying and promoting a human rights approach to data protection and privacy, and for the purpose of providing a comprehensive policy concerning data protection and privacy for the Secretariat of the United Nations, including all its activities at Headquarters and away from Headquarters, promulgates the following:

I. General provisions

Section 1
Purpose

1.1 The present policy is designed:

(a) To ensure that personal data, as well as "non-personal data in a sensitive context", as defined below, is processed in a non-discriminatory, gender-sensitive manner, for purposes consistent with United Nations mandates and in a manner that respects the rights of individuals and groups as set forth herein;

(b) To implement the Personal Data Protection and Privacy Principles adopted by the High-level Committee on Management of the United Nations System Chief Executives Board for Coordination;[1]

(c) To be a basis for harmonizing data protection and privacy policies across United Nations system organizations, consistent with best practices;

(d) To provide transparency, establish the safeguards necessary to ensure that the United Nations processes in a responsible fashion personal data, as well as "non-personal data in a sensitive context", as defined below, and manages related risks;

(e) To create an environment that facilitates the flow, use and sharing of data in furtherance of United Nations mandates;

(f) To support the 2030 Agenda for Sustainable Development and the decade of action and delivery for sustainable development.

[1] Adopted on 11 October 2018.

1.2 The processing of non-personal data other than “non-personal data in a sensitive context”, as defined below, falls outside the scope of the present bulletin.

Section 2
Definitions for the purposes of the present bulletin

Personal data

2.1 Personal data is information, in any form, that relates to an identified or identifiable natural person.

Sensitive personal data

2.2 Sensitive personal data is a type of personal data that relates to one of the following: ethnic origin; migration status; political, religious or other opinions, beliefs or affiliations; personal financial information; trade union membership; personal genetic or biometric data uniquely identifying individuals; health; gender identity; or sexual orientation.

Non-personal data in a sensitive context

2.3 Non-personal data in a sensitive context is information, in any form, that, while not relating to an identified or identifiable natural person, may, by reason of its sensitive context, put certain individuals and groups at risk of harm, including vulnerable or marginalized individuals and groups of individuals, such as children.

Data subject

2.4 The data subject is any identified or identifiable natural person to whom personal data that are being processed by or on behalf of the Secretariat relate, including but not limited to a staff member, individual contractor or consultant, other United Nations personnel, an attendee at an official meeting or a beneficiary of assistance.

Identifiable natural person

2.5 An identifiable natural person is a natural person who can be directly or indirectly identified by means likely to be used, such as reasonably available expertise, resources and time, as well as data already available.

Consent

2.6 Consent is any freely given, specific and informed indication of an agreement by the data subject to the processing of their personal data.

Data steward

2.7 The data steward is the head of each entity,[2] unless otherwise determined by the Secretary-General. In relation to data that fall within the scope of the present bulletin and are shared across Secretariat entities, including through Secretariat-wide enterprise systems and controls, or that otherwise relate to several entities, the Chief Data Protection and Privacy Officer will assist the Secretary-General in identifying the relevant data steward(s).

[2] “Head of entity” has the same meaning as in footnote 1 of Secretary-General’s bulletin ST/SGB/2019/2 on delegation of authority in the administration of the Staff Regulations and Rules and the Financial Regulations and Rules, or its successor.

Data processor

2.8 The data processor is anyone who processes data that fall within the scope of the present bulletin and who does so under the supervision or direction, or on behalf, of the data steward(s).

Processing of data

2.9 Data processing is any operation or set of operations that is performed on data or on sets of data, irrespective of the technology and processes used, including by automated means, by or on behalf of the Secretariat, including but not limited to collecting, registering, recording, structuring, storing, adapting, altering, cleaning, filing, retrieving, consulting, using, disseminating, disclosing, transferring, sharing, copying, making available, erasing and destroying.

Automated decision-making

2.10 Automated decision-making is the process of making a decision through the processing of data by automated means and without review or intervention by a natural person.

Data breach

2.11 A data breach is the loss, destruction, alteration, access, acquisition or use for unauthorized purposes of data that fall within the scope of the present bulletin, caused by accidental or unlawful disclosure, that compromises the confidentiality, security, availability or integrity of the data.

II. Governance and oversight

Section 3
Data Governance Group

The Secretary-General will designate the senior officials who will support him or her on general oversight of the implementation of the present bulletin and related administrative issuances on data protection and privacy of the Secretariat, as well as in promoting policy developments in relation thereto. Such designated officials will comprise the Data Governance Group.

Section 4
Chief Data Protection and Privacy Officer

A Chief Data Protection and Privacy Officer is appointed or designated by the Secretary-General, reports directly to him or her on matters pertaining to the present bulletin and is responsible for:

(a) Providing independent and impartial advice and support to the Secretary-General and data stewards on the measures to be taken to ensure compliance with the present bulletin and other related administrative issuances, including in relation to data impact assessments under section 11 below;

(b) Establishing and maintaining the centralized reporting mechanism for the purpose of receiving and disseminating to the relevant data steward requests by data subjects under section 17 below;

(c) Chairing the Data Protection and Privacy Committee pursuant to section 5 below;

(d) Developing mandatory and other training for all staff members and other personnel on the present bulletin and other related administrative issuances;

(e) Maintaining documentation of information provided by data stewards, including data inventories, data transfer agreements, specific instances of data-sharing with third parties, data impact assessments, data breach notifications and responsive actions taken in respect thereof, and requests by data subjects;

(f) Liaising with data protection focal points in each entity, as required;

(g) On their own initiative or upon request by a data steward, reviewing any processing of data that fall within the scope of the present bulletin;

(h) Advising on measures to be taken to ensure compliance with the present bulletin in relation to Secretariat-wide enterprise systems and controls and liaising with technical focal points for each such system;

(i) Assisting the Secretary-General in determining the relevant data steward(s) in relation to data that are shared across Secretariat entities, including through Secretariat-wide enterprise systems and controls, or that otherwise relate to several entities, pursuant to section 2.7 above;

(j) Monitoring and reporting to the Secretary-General on compliance with the present bulletin and assisting the Secretary-General with the Secretariat's reporting obligations on matters related to data protection and privacy;

(k) Taking any other action necessary for compliance with and implementation of the present bulletin and any other related administrative issuances.

Section 5
Data Protection and Privacy Committee

5.1 A Data Protection and Privacy Committee will be chaired by the Chief Data Protection and Privacy Officer and composed of staff members appointed by the Chef de Cabinet after consultation with the relevant heads of entities. Such staff members will be appointed from among those with relevant skills and expertise from across the Secretariat and will serve in an independent advisory capacity.

5.2 Pursuant to section 19 below, the Data Protection and Privacy Committee will independently and impartially review determinations by data stewards on requests concerning the processing of personal data and make a recommendation to the Under-Secretary-General for Management Strategy, Policy and Compliance regarding such requests.

Section 6
Data stewards

6.1 Data stewards will be responsible for:

(a) Establishing procedures internal to their respective entities, such as standard operating procedures with regard to data protection and privacy, covering all relevant aspects of the present bulletin;

(b) Specifying, in accordance with section 11.1 below, with respect to data that fall within the scope of the present bulletin, the purposes and means of the processing of data, the content and use of the data being processed, and any mitigation measures;

(c) Conducting data impact assessments whenever the conditions under section 11.2 below are met;

(d) Pursuant to section 12 below, ensuring appropriate safeguards in relation to transfers of data outside the United Nations;

(e) Providing information to data subjects pursuant to section 13 below or upon a request received pursuant to section 17 below;

(f) Ensuring, pursuant to section 14 below, the retention and periodic deletion of personal data maintained by the respective entity;

(g) Pursuant to section 15 below, notifying data subjects of data breaches;

(h) Pursuant to section 18 below, making determinations and taking action, as appropriate, on requests concerning the processing of personal data;

(i) Establishing and maintaining an inventory and regularly providing an overview of such inventory to the Chief Data Protection and Privacy Officer concerning: data that fall within the scope of the present bulletin, significant data transfer arrangements, data impact assessments, data breach notifications and responsive actions taken in respect thereof;

(j) Designating one or more data protection focal points;

(k) Ensuring that all staff members and personnel complete regular mandatory training on data protection and privacy;

(l) Taking any other action necessary within the entity for compliance with and implementation of the present bulletin and any other related issuance.

6.2 If the data processing activity is carried out under the authority of more than one data steward, responsibility for taking the actions set forth in section 6.1 above will be determined in accordance with section 2.7 above.

Section 7
Data protection focal points

7.1 For each United Nations Secretariat entity, the data steward will designate one or more data protection focal points to provide support in carrying out the functions and responsibilities set forth in section 6 above.

7.2 In supporting the data stewards, data protection focal points should liaise with the Chief Data Protection and Privacy Officer as appropriate.

Section 8
Monitoring, accountability and compliance

8.1 Responsibilities of the data steward(s), data processor(s), data focal point(s) and Chief Data Protection and Privacy Officer under the present bulletin will be monitored through compacts with senior officials or the Performance Management and Development System, as appropriate.

8.2 In accordance with its mandate, the Office of Internal Oversight Services may from time to time conduct data protection and privacy audits to evaluate overall compliance with the present bulletin in accordance with the applicable regulations, rules and relevant administrative issuances.

III. Data processing

Section 9
Principles of data processing

9.1 Personal data, including sensitive personal data, will be processed in accordance with the principles outlined in the present section. Non-personal data in a sensitive context will also be processed in accordance with these principles, insofar as they are applicable in the circumstances.

Fair and legitimate processing

9.2 Personal data may be processed if at least one of the following legal bases applies:

(a) The processing is with the consent of the data subject;

(b) The processing is required for the performance or conclusion of an agreement with the data subject or with another party for the benefit of the data subject;

(c) The processing is essential for the protection of the vital interests of the data subject, or the best interests of the data subject if the data subject is a child;

(d) The processing is necessary for the performance of investigations, audits, the pursuit or defence of legal claims, or the proper administration of justice;

(e) The processing is necessary to perform a mandate received from intergovernmental bodies, or for the undertaking of functions under the Charter of the United Nations or as provided in the Staff Regulations and Rules or the Financial Regulations and Rules of the United Nations or any administrative issuance of the United Nations;

(f) The processing is necessary to perform obligations in an agreement with a third party, provided that such agreement or the administration of such agreement affords an appropriate level of security and protection for the personal data in a manner at least equivalent to the principles in the present bulletin;

(g) The processing is necessary to fulfil an overriding legitimate interest of the United Nations in using the personal data.

Purpose specification

9.3 Personal data will be processed only for the purposes that are specified by the data steward under section 6.1 (b) above and that are permitted pursuant to one or more of the relevant legal bases for data processing under section 9.2 above.

Proportionality and necessity

9.4 The processing of personal data shall be relevant, limited and adequate to what is necessary in relation to the purposes specified in accordance with section 9.3 above.

Retention

9.5 Subject to any rules or policies on the retention of records to be preserved for their administrative, fiscal, legal, scientific, historical or informational value, and in accordance with section 14 below, personal data will be retained only for the amount of time that is necessary for the purposes specified under section 9.3 above.

Accuracy

9.6 Subject to the obligations of staff members to provide accurate personal information under the Staff Regulations and Rules of the United Nations and relevant administrative issuances, personal data will be maintained as accurately as possible and, where necessary, updated to fulfil the specified purposes.

Confidentiality

9.7 Personal data will be handled in accordance with Secretary-General's bulletin ST/SGB/2007/5 on record-keeping and the management of United Nations archives, as may be amended or superseded, and any other relevant regulation, rule and administrative issuance concerning information sensitivity, classification and handling that is applicable to the Secretariat.

Security

9.8 Personal data will be processed in a manner designed to protect its security, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.

Transparency

9.9 In accordance with section 13, as appropriate and whenever possible, information will be provided to data subjects in relation to the processing of data relating to them.

Transfers

9.10 Personal data may be transferred outside the United Nations only provided that the receiving party affords an appropriate level of security and protection for the personal data in a manner at least equivalent to the principles in the present bulletin.

Section 10
Data protection and privacy by design

10.1 In consultation with the Chief Data Protection and Privacy Officer, the Office of Information and Communications Technology will set and approve relevant technical safeguards, as well as provide advice on the adoption of organizational safeguards, to ensure that the requirements of the present bulletin can be met to the maximum extent possible throughout the entire life cycle of data processing. In relation to systems for which they are responsible, data stewards will ensure that such technical safeguards are embedded within all systems that process personal data.

10.2 Relevant technical safeguards may include anonymization, pseudonymization, encryption, differential privacy and other privacy-enhancing technologies. Organizational safeguards may include administrative procedures and policies outlined in the present bulletin.

Section 11
Data mapping and data impact assessment

11.1 In relation to all data that fall within the scope of the present bulletin, data stewards will conduct a data-mapping exercise consisting of the review of all programmed activities under their purview to specify the purposes and means of the processing of data in connection with such activities, the content and use of the data being processed, and any mitigation measures that may be necessary to ensure that such processing is consistent with the principles in section 9 above. Such a data-

mapping exercise will be conducted periodically, and at least once every three years. In addition, any new or substantially modified programmed activities will be similarly subject to such review.

11.2 When the processing of data specified in accordance with section 11.1 involves any of the following circumstances, the data steward will conduct a data impact assessment to identify and assess the potential risks, harms and benefits linked to the processing of such data and the appropriate measures to prevent or mitigate any risks or harms identified:

(a) The processing of sensitive personal data;

(b) The processing of non-personal data in a sensitive context;

(c) The processing of large amounts of personal data;

(d) The processing of data involving significant merging, matching and manipulation of multiple data sets;

(e) Automated decision-making that would result in decisions significantly affecting data subjects;

(f) The use of artificial intelligence, blockchain or other similar emerging technologies to process data;

(g) The processing of data otherwise presents serious risks of harm to one or more individuals or groups of individuals.

11.3 The data impact assessment should normally contain:

(a) A general description of the envisaged system, project, policy or data-sharing arrangement involving processing of data that fall within the scope of the present bulletin;

(b) An assessment of the purpose of the processing, including its potential benefits to the programmed activities and, as a result thereof, to data subjects;

(c) An assessment of the risks and harms to data subjects and other individuals or groups potentially affected;

(d) An assessment of the necessity and proportionality of the processing operations in relation to the specified purpose for such data processing;

(e) A general description of the safeguards, security and other measures already in place or proposed to ensure the protection of the data;

(f) Identification of the safeguards and security and other measures that are already in place or that it would be advisable to adopt in order to prevent and mitigate any risks and harms to data subjects and other individuals or groups potentially affected, including the option of not processing data in the given circumstances.

11.4 The data steward may consult, as appropriate, the Chief Data Protection and Privacy Officer during the data impact assessment to ensure consistency in approach across the Secretariat and to obtain any technical or other assistance required.

11.5 On the basis of such data impact assessment and any advice received from the Chief Data Protection and Privacy Officer, the data stewards will determine the appropriate course of action to ensure that data that fall within the scope of the present bulletin are processed in accordance with its requirements. Such action may include making any appropriate changes to the implementation of the programmed activities or to the methods or tools used for the handling of such data; it may also include the decision not to process such data, or not to further process such data.

Section 12
Transfers and sharing outside the United Nations

12.1 When a Secretariat entity transfers or shares data that fall within the scope of the present bulletin outside the United Nations, the data steward must make reasonable efforts to ensure that the receiving party affords appropriate protection for such data in a manner at least equivalent to the principles in the present bulletin.

12.2 The data steward may ensure such protection through a standing agreement, transactional agreements or other reasonable means. The Chief Data Protection and Privacy Officer will develop standard model arrangements for such purpose.

Section 13
Provision of information to data subjects

13.1 Unless providing such information would be contrary to the purpose of data processing or to the confidentiality obligations of the data steward, and except in cases where data subjects already possess the relevant information, data stewards should make available general information to data subjects as to:

(a) The legal basis and specified purpose of processing of personal data under sections 9.2 and 9.3 above;

(b) The safeguards applicable to such data processing;

(c) The types of data being processed;

(d) The source of data;

(e) Whether data processing involves automated decision-making that would result in decisions significantly affecting them;

(f) If data are being transferred, the recipient of the transfer and the purpose therefor;

(g) The procedures for making requests concerning the processing of their personal data pursuant to section 17 below.

13.2 Such information should preferably be provided at the time of the collection of personal data or the transfer of such data outside the United Nations, including through individual or publicly available notices, or consent forms.

Section 14
Retention of personal data and non-personal data in a sensitive context

14.1 Data stewards will establish internal processes in their respective entities for the periodic deletion of personal data and non-personal data in a sensitive context that is no longer needed for any purpose that is consistent with a legal basis for data processing under section 9.2.

14.2 The Chief Data Protection and Privacy Officer may issue recommendations for standardizing the processes concerning the periodic deletion of data that fall within the scope of the present bulletin.

14.3 Such processes will be established, and such recommendations made, in a manner consistent with established processes for the retention of records in accordance with Secretary-General's bulletin ST/SGB/2007/5 on record-keeping and the management of United Nations archives, as may be amended or superseded, or any other relevant administrative issuance.

Section 15
Data breach management

15.1 Data stewards will inform and thereafter consult with the Chief Data Protection and Privacy Officer and the Office of Information and Communications Technology to manage any suspected or actual data breaches. Data stewards will maintain a register of all confirmed data breaches and of the mitigation measures adopted in response thereto.

15.2 The Office of Information and Communications Technology will adopt technical procedures to prevent and mitigate data breaches in information systems. The relevant data steward(s) will be responsible for notifying data subjects, when appropriate, of any data breach and of the mitigation measures adopted.

IV. Rights and remedies in relation to personal data

Section 16
Rights of data subjects

The rights of data subjects to information on, access to, rectification and deletion of and objection to the processing of personal data relating to them will be exercised in accordance with the procedures and subject to the conditions set out in sections 17, 18 and 19 below.

Section 17
Requests concerning processing of personal data

17.1 With respect to concerns about the processing of personal data relating to them, individuals may submit one or more of the requests described in the present section.

17.2 When submitting any such requests, individuals shall in each instance show that their request is well founded.

Request as to whether personal data is being processed

17.3 Individuals may address a request to the centralized reporting mechanism to ascertain whether personal data relating to them are in fact being processed by the Secretariat. In making such requests, individuals shall, at a minimum, state the circumstances in relation to which they have reason to believe that the Secretariat is processing personal data relating to them.

Requests by data subjects

17.4 Individuals who are data subjects may address a request, in relation to a specific instance of processing of personal data relating to them, for information as to:

(a) The legal basis and specified purpose of processing of personal data under sections 9.2 and 9.3 above;

(b) The safeguards applicable to such data processing;

(c) The types of data being processed;

(d) The source(s) of data;

(e) The applicable retention period;

(f) Whether data processing involves automated decision-making that would result in decisions significantly affecting them;

(g) Whether data are being transferred outside the United Nations and, if data are being transferred, the recipient of the transfer and the purpose therefor.

17.5 Staff members may view their official status files in accordance with administrative instruction ST/AI/108 on annual inspection of official status file, or any subsequent administrative issuance. Other data subjects may request access to a copy of personal data relating to them.

17.6 Staff members may request rectification of their personal data in accordance with administrative instruction ST/AI/2010/2 on request for rectification of date of birth or of other personal data, or any subsequent administrative issuance. Other data subjects may request rectification or completion of inaccurate or incomplete personal data.

17.7 Data subjects may request the deletion of personal data relating to them.

17.8 Data subjects may request that the Secretariat cease or restrict the processing of personal data relating to them.

Centralized reporting mechanism

17.9 The Chief Data Protection and Privacy Officer will establish and maintain a centralized reporting mechanism for the purpose of receiving and recording the requests described in sections 17.3 to 17.8 above. The Chief Data Protection and Privacy Officer will establish a standard form for such requests.

17.10 The Chief Data Protection and Privacy Officer will disseminate each such request to the relevant data steward. In the event that a doubt arises as to the relevant data steward, the Chief Data Protection and Privacy Officer will identify the relevant data steward for the purpose of handling the request.

17.11 The available method for filing a request through the centralized reporting mechanism should normally be made public in the privacy notice included on United Nations websites, as well as in any applicable data protection and privacy consent forms pursuant to section 13 above.

Section 18
Determination by the data steward on requests concerning the processing of personal data

18.1 The data steward will determine whether to accede to any request made under section 17.

18.2 The data steward may ask for further details or substantiating evidence to enable the making of such determination on the request.

18.3 The data steward shall deny a request and such denial will be without further consideration or recourse if the content, use or means of the processing of data falls outside the purview of the Secretariat (for example, when the content, use or means of the processing of data is directly determined by the General Assembly, the Security Council, the Economic and Social Council, the International Court of Justice or any of their subsidiary organs, including sanctions bodies, investigative bodies, accountability mechanisms and criminal tribunals). Such denial is not subject to section 19 below.

18.4 The data steward may deny a request for the sole reason that it relates to the processing of data for any of the following specified purposes:

(a) The provision of legal advice;

(b) The provision of mutual legal assistance or judicial cooperation to Member States or international courts, tribunals or accountability mechanisms;

(c) Investigations concerning allegations of criminal conduct or other misconduct, including fraud, corruption, conflicts of interest, sexual harassment, sexual abuse or sexual exploitation;

(d) Protection against retaliation;

(e) The financial disclosure programme;

(f) The advisory functions of the Ethics Office;

(g) Internal audits, inspections and evaluations;

(h) Fact-finding, monitoring or investigation activities conducted by the Secretariat in relation to breaches of international human rights law or international humanitarian law;

(i) Fact-finding or investigation activities in relation to specific incidents undertaken by boards of inquiry or other investigative or fact-finding bodies established by or under the authority of the Secretary-General;

(j) Any activities carried out by the Secretariat in its support of sanctions bodies, investigative bodies, accountability mechanisms and criminal tribunals established by the General Assembly, the Security Council or their subsidiary organs;

(k) Ongoing or anticipated litigation before the United Nations Dispute Tribunal or the United Nations Appeals Tribunal;

(l) Otherwise where the United Nations has a duty of confidentiality in respect of the information concerned.

18.5 Data stewards may accede to any request if they have determined, in their discretion, that the requestor has demonstrated that such request is well founded and if they have determined, in their discretion, that such request is consistent with the applicable legal framework and is not abusive, fraudulent or too onerous to comply with given existing resources, and that granting such request would not impair the legal basis or the specific purpose of the data processing; does not impair the execution of mandates of the Organization; would not jeopardize the security, privacy, safety and health of individuals and groups; would not jeopardize other rights of individuals and groups; and would not frustrate other overriding legitimate interests of the United Nations.

18.6 The determination by the data steward of whether to accede to requests will be communicated in writing to the requestor. Whenever possible and appropriate, the reasons for denying a request will also be given.

Section 19
Review by the Data Protection and Privacy Committee

19.1 In cases of denial of a request by the data steward, in whole or in part, for reasons other than those specified under section 18.3 above, the requestor may request a review of such denial by the Data Protection and Privacy Committee by making such request for review to the Chief Data Protection and Privacy Officer on a form prescribed by the Chief Data Protection and Privacy Officer within 30 days following receipt of the data steward's determination. The Chief Data Protection and Privacy Officer may, for good cause shown by the requestor, extend this time limit.

19.2 The Data Protection and Privacy Committee will review the determination by the data steward and make a recommendation to the Under-Secretary-General for Management Strategy, Policy and Compliance regarding such request.

19.3 On the basis of the recommendation received, the Under-Secretary-General for Management Strategy, Policy and Compliance will make a final decision on such request.

19.4 Such final decision will be communicated in writing to the requestor and to the data steward.

19.5 Where such final decision constitutes an administrative decision adversely affecting the rights of a staff member and producing direct legal consequences in relation to the terms of that person's employment as a staff member, the staff member in question may have rights regarding such decision under article XI of the Staff Regulations and chapter XI of the Staff Rules. In such cases, the Data Protection and Privacy Committee constitutes a technical body within the meaning of Staff Rule 11.2. Accordingly, the decision by the Under-Secretary-General for Management Strategy, Policy and Compliance pursuant to section 19.3 above will not require management evaluation.

19.6 In relation to requestors who are not staff members, a challenge to the decision made by the Under-Secretary-General for Management Strategy, Policy and Compliance on the request would be subject to such method of amicable resolution and dispute settlement as determined by the Secretary-General under any contract governing their relationship with the United Nations, or as set forth in a separate administrative issuance.

V. Final provision

Section 20
Entry into force and periodic review

20.1 The present bulletin shall enter into force on the date of its issuance.

20.2 The present bulletin shall be regularly assessed for any necessary updates.

(*Signed*) António **Guterres**
Secretary-General