UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION

ST

UNIDO SECRETARIAT

DGB/2023/05
14 March 2023

Distribution: All personnel at Headquarters
and established offices
and Permanent Missions

# DIRECTOR GENERAL'S BULLETIN

## UNIDO Policy on the Protection of Personal Data

1. The purpose of this Director General's bulletin is to promulgate the UNIDO Policy on the Protection of Personal Data.

2. The custodian of the Policy is the Managing Director of the Directorate of Corporate Services and Operations (COR), who is responsible for monitoring the overall compliance with the Policy.

3. All personnel of UNIDO at Headquarters and in the field are required to comply with the Policy.

4. This bulletin takes effect on the date of its issuance.

**UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION**

# UNIDO POLICY ON THE PROTECTION OF PERSONAL DATA

## Contents

# UNIDO POLICY ON THE PROTECTION OF PERSONAL DATA

## I. Purpose and Rationale

1. UNIDO is often required to collect, use and otherwise process personal data in the course of its activities and operations and in the implementation of its mandate to promote inclusive and sustainable industrial development (ISID). The processing of personal data may also include the sharing of such data with implementing partners and other third parties.

2. The processing of personal data poses inherent risks, such as the accidental or unauthorized loss or disclosure of the data. Personal data protection is consequently essential to safeguard the right to privacy of individuals in relation to the processing of their personal data.

3. The purpose of the present Policy (hereinafter "the Policy") is to safeguard the right to privacy by ensuring that personal data processed by or on behalf of UNIDO enjoys an appropriate level of protection. To this end, the Policy lays down ten principles governing the protection of personal data, which apply to all personal data contained in any form and processed in any manner. The Policy further provides an overview of specific roles and responsibilities in implementing the provisions of the Policy.

4. The Policy is based on the UN system-wide *Principles on Personal Data Protection and Privacy*, as adopted by the High-Level Committee on Management (HLCM) in 2018[1]. Accordingly, it aims to contribute to the harmonization of standards for the protection of personal data across the United Nations system. The Policy also aims to facilitate the accountable processing of personal data, and, in so doing, to foster respect for human rights, in particular the right to privacy. Consistent with this Policy, UNIDO further seeks to ensure that personal data is processed in a non-discriminatory, gender-sensitive manner.

## II. Scope

5. The Policy applies to the Secretariat of UNIDO and to all offices of UNIDO as a single organization.

6. The Policy applies to all UNIDO personnel at Headquarters and in the field. All personnel are required to comply with the Policy. Non observance of the responsibilities provided for under the Policy may result in disciplinary or administrative action.

---

[1] Available at: https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf. Due regard is also paid to the *Guidelines for the Regulation of Computerized Personal Data Files*, adopted by the UN General Assembly in its resolution 45/95, and to other international instruments concerning the protection of personal data.

7. Nothing contained in or relating to this Policy, or done pursuant to it, shall be construed as a waiver of any of the privileges and immunities enjoyed by UNIDO under national or international law.

## III. Definitions

8. ***Anonymization*** means a process of using all reasonable means to strip, disguise or otherwise convert information that could be used to identify an individual from a data set into anonymous data, such that it cannot be traced back or linked to an individual(s) or group(s) of individuals either directly or by deduction.

9. ***Consent*** means any freely given, specific, explicit, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

10. ***Data controller*** means natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

11. ***Data processing*** or ***processing*** means any operation or set of operations performed on personal data, whether or not by automatic means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

12. ***Data protection impact assessment (DPIA)*** means a standardized assessment tool and process based on the principles set out in this Policy that assesses the impact of the envisaged processing activities on the protection of personal data and on the rights of data subjects. Such assessment aims to identify remedial actions as necessary in order to avoid or minimize any adverse impact.

13. ***Data subject*** means a living individual, who can be identified, directly or indirectly, through the personal data collected and/or processed by or on behalf of UNIDO.

14. ***Data transfer agreement*** means an agreement between UNIDO and a third party that states the terms and conditions governing the transfer of personal data to the third party, including which data components are to be transferred, the mode of transfer, how the data may be used, data security measures to be implemented, and other related issues.

15. ***Organizational unit*** means a directorate, division/services, office or unit of UNIDO at Headquarters or in the field.

16. ***Personal data*** means any information relating to a living individual, by which that individual may be identified or is identifiable, either directly or indirectly. It is important to note that the definition of personal data now specifically includes information such as identification numbers, location data and online identifiers. In practice, any data about a living person who can be identified from the data available (or potentially available) will count as personal data. This will include reversibly anonymized (pseudonymized) data i.e., replacing any identifying characteristics of data with a value which does not allow the data subject to be directly identified (pseudonym). Where a pseudonym is used, it is often possible to identify the data subject by analyzing the underlying or related data.

17. ***Personal data breach*** or ***data breach*** means a breach of security leading to the accidental or unauthorized destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

18. ***Personal data security*** means the protection of the confidentiality, integrity and availability of personal data.

19. ***Personal data transfer*** or ***data transfer*** means any action that makes personal data accessible or otherwise available to another party, other than the data subject, regardless of the media and format (electronic or physical). The movement of data and the provision of access to data to other individuals within UNIDO is not a personal data transfer. Personal data transfer includes transfers within a country as well as transfers from the country where the data was originally collected to another country or countries.

20. ***Profiling*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

21. ***Pseudonymization*** means any technical process under which personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

22. ***Sensitive personal data*** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union/staff association membership, genetic data and biometric data capable of uniquely identifying a natural person, data concerning health, or data concerning an individual's sex life or sexual orientation.

23. ***Technical controls*** mean the hardware and software components that protect a system against cyberattacks. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.

24. ***Third party*** means a natural or legal person unrelated to UNIDO, including any implementing partner, public authority, agency, grant beneficiary, vendor, or subcontractor.

25. ***UNIDO personnel*** or ***personnel*** means, collectively, staff members of UNIDO, holders of individual service agreements, interns, volunteers, partner-experts and other costs-free experts seconded or loaned to UNIDO.

## IV. Personal Data Protection Principles

26. The following principles shall govern the protection of personal data by and within UNIDO:

(a) Fair and legitimate processing

Personal data shall be processed in a fair manner, and on the basis of one or more of the following legitimate bases:

(i) The consent of the data subject;
(ii) The vital interests of the data subject or another individual;
(iii) The mandate or the legal framework of UNIDO, including its Constitution and applicable decisions of its policymaking organs;
(iv) A legal obligation to which UNIDO is subject;
(v) A contract that has been or will be concluded with the data subject, including a contract of employment;
(vi) The legitimate interests of UNIDO consistent with its mandate.

(b) Purpose specification

Personal data shall be processed for one or more specific purpose, consistent with the mandate of UNIDO. Personal data shall not be processed in ways that are incompatible with such purposes.

(c) Security

Appropriate organizational, administrative, physical and technical safeguards and procedures shall be implemented to protect the security of personal data from unauthorized or accidental access, damage, loss or other risks presented by data processing. Having regard to the cost of implementation, these safeguards and procedures may include technologies and tools to enhance the protection of particularly sensitive personal data (privacy by design and by default).

(d) Confidentiality

Personal data shall normally be classified as confidential information. The confidentiality and level of sensitivity of personal data shall be borne in mind at all times when processing personal data. Personal data shall also be filed and stored in such a way that it is accessible only to authorized personnel and is transferred only through the use of protected means of communication.

(e) Proportionality and necessity

The processing of personal data shall be relevant, limited and adequate to what is necessary in relation to the purpose(s) of the processing.

(f) Retention

Personal data shall be retained only for the time that is necessary for the specified purpose or in accordance with the UNIDO record retention schedule.

(g) Transparency

The processing of personal data shall be carried out with transparency to data subjects, as appropriate and whenever possible. This transparency shall include the provision of information about the processing of the personal data, and information on how to exercise rights under the Policy, including on how to object to the processing, and on how to request access to, or verification, rectification and/or erasure/deletion of that personal data, insofar as the specified purpose for which personal data is processed is not frustrated.

(h) Accuracy

Personal data shall be accurate and, where necessary, up to date to fulfill the specified purposes.

(i) Personal data transfers

In carrying out its mandated activities, UNIDO may, as data controller, transfer personal data to a third-party data processor, provided that, under the circumstances, UNIDO has satisfied itself that the third party affords appropriate protection for the personal data. Unless there are satisfactory reasons not to do so, prior to transferring personal data to a third party, UNIDO should seek to sign a data transfer agreement or, as appropriate, include standard data protection clauses within broader agreements or contracts.

(j) Accountability

Adequate policies, procedures and processes shall be in place to ensure adherence to this Policy.

## V. Rights of Data Subjects

27. Under this Policy, the rights of data subjects are as follows:

(a) Right to be informed

The data subject has a right to be informed of what personal data is being collected and for what purpose, how the data will be used, for how long and by whom, where the data will be stored/kept and, if applicable, with whom the data will be shared.

(b) Right of access

Provided their identity is verifiable, the data subject may request to be informed of which personal data relating to them has been collected and stored, how the personal data was collected, and for what purpose. Such requests shall be submitted in writing. Disclosure of personal data must not be automatic.

(c) Right to rectification

Provided their identity is verifiable, and depending on the purposes of the processing, the data subject may request that incorrect or incomplete personal data be corrected or supplemented. Upon verification, UNIDO will make the necessary change(s). Under certain circumstances, a request for rectification may be refused, for example, if it is unfounded or excessive.

(d) Right to erasure/deletion

Provided their identity is verifiable, the data subject may request that their personal data be erased or deleted if the processing of such personal data has no legitimate basis, or if the legitimate basis has ceased to apply. The same applies if the purpose of the data processing has lapsed or has ceased to be applicable. However, the right to erasure does not apply, and the personal data will continue to be retained:

(i) For the implementation of the mandate of UNIDO;
(ii) For historical, statistical and/or scientific purposes;
(iii) For the establishment, exercise or defense of legal claims; or
(iv) For other legitimate interests.

(e) Right to object

Provided their identity is verifiable, the data subject may object at any time, on compelling and legitimate grounds relating to their particular situation, to the processing of their personal data.

(f) Right in relation to automated decision-making and profiling

Provided their identity is verifiable, the data subject may object to a decision based solely on automated processing without human intervention, such as the use of profiling, and which produces material and adverse legal or other effects on them, unless the processing is carried

out with consent, is necessary for entering into or performance of a contract between the data subject and UNIDO, or is necessary for other legitimate interests.

## VI. Roles and Responsibilities

28. Director General: The Director General, as chief administrative officer of UNIDO, has the ultimate responsibility for establishing, promulgating and implementing an effective organizational data protection policy or framework.

29. Managing Director, Corporate Services and Operations (MD/COR): The MD/COR bears overall responsibility for the implementation and monitoring of, and compliance with, this Policy and related administrative issuances.

30. UNIDO Data Protection Officer (DPO): The DPO is responsible for:
(a) monitoring and advising on all aspects of compliance with the Policy, as well as for relevant awareness-raising activities and for the training of UNIDO personnel;
(b) acting as point of contact with regard to this Policy, including in the case of requests from data subjects regarding the processing of their personal data and the exercise of their rights under the Policy, and in the case of personal data breaches;
(c) coordinating the response in case of personal data breaches, in consultation with relevant organizational units, where required;
(d) coordinating the Data Protection Impact Assessments (DPIA) performed by the heads of organizational units and providing advice, as appropriate, where a DPIA has been carried out.

31. Managing Directors: Managing Directors are responsible for the protection of personal data within their respective Directorates.

32. Heads of Organizational Units: The heads of organizational units are responsible for the identification and labelling of personal data to which their organizational units have access. They shall, in relation to all personal data that falls within the scope of this Policy, conduct and regularly repeat a data mapping exercise in consultation and coordination with the DPO and conduct DPIAs whenever the conditions under paragraph 44 are met. They are also responsible for establishing processes for the retention and deletion of personal data as described in Section VII and for ensuring appropriate protection whenever the data is transferred to a third party as set out in Section X.

33. UNIDO Personnel: All UNIDO personnel are responsible for taking reasonable and appropriate steps to protect the personal data to which they have access. Personnel also have the duty to report any incident involving an actual, potential, or suspected personal data breach to the DPO, as well as to cooperate with investigations related to personal data breaches and with requests by data

subjects. Personnel may be required from time to time to complete relevant data protection training.

## VII. Retention of Personal Data

34. The heads of organizational units shall establish internal processes in their respective units for the periodic deletion of personal data that is no longer needed for any purpose that is consistent with a legitimate basis for data processing.

35. Such processes shall be consistent with established processes for the retention of records in accordance with relevant administrative issuances on record-keeping and the management of UNIDO's archives.

## VIII. Requests by Data Subjects and Reporting of Data Breaches

36. Requests by data subjects exercising their rights under this Policy shall follow the procedures set out in paragraphs 21 to 24 of the UNIDO Information Disclosure Policy.[2] All requests by data subjects pertaining to their personal data addressed to the heads of organizational units shall be handled appropriately in consultation with the DPO and, where necessary, the MD/COR.

37. All UNIDO personnel shall report any incident involving an actual, potential, or suspected data breach (hereinafter referred to as "incident") as soon as possible upon becoming aware of the incident. Incidents should be reported directly to the DPO (personal-data-breach@unido.org).

38. External data subjects may report incidents by following the guidance published on the external UNIDO website.

39. The report should include all information available in relation to the incident at the time of notification, including the date and time of the discovery, nature and location of the affected personal data, any available evidence of the incident and details of the date of the potential breach.

40. The DPO shall coordinate UNIDO's response to an incident report, in consultation with relevant organizational units, which may vary from case to case.

41. If the incident involves allegations of fraud or other misconduct on the part of UNIDO personnel, the allegation shall be referred to the Office of Evaluation and Internal Oversight (EIO) in line with the Charter of EIO and the Investigation Policy.

[2] DGB/2021/17 dated 17 December 2021, or the latest iteration thereof.

42. In case the DPO establishes, based on the technical assessment and recommendation of the relevant organizational unit, that a data breach has occurred, the DPO shall notify the affected data subject(s) accordingly.

43. The DPO shall maintain a Register of Personal Data Breaches containing a record of all incidents reported.

## IX. Data Protection Impact Assessments (DPIA)

44. When the processing of personal data is likely to involve high risks to the rights of any data subjects, in particular when elaborating a new system or project, a DPIA shall (and in other cases may) be conducted by the head of the responsible organizational unit, prior to the processing, to identify the risks and any corresponding remedial measures.

45. The DPO should be informed of any DPIA carried out and provided with a copy of the DPIA.

## X. Transfers and Sharing Outside of UNIDO

46. When UNIDO (as a data controller) transfers or shares personal data with a third party outside UNIDO, the head of the relevant organizational unit must ensure that the receiving third party affords appropriate protection for such data at least equivalent to the principles of personal data protection as set out in this Policy.

47. The head of the organizational unit may ensure such protection through a data transfer agreement or, as appropriate, through including standard data protection clauses within broader agreements or contracts. The DPO shall develop a standard data transfer agreement or agreements for such purpose.

## XI. Audit and Evaluation

48. The present Policy shall be subject to audit and/or evaluation by the Office of Evaluation and Internal Oversight (EIO) in accordance with the provisions of the Charter of EIO,[2] the Internal Audit Policy,[3] and the Evaluation Policy.[4] EIO may provide such assurance services in connection with the present Policy as it considers to be necessary and appropriate.

[2] DGB/2020/11 or the latest iteration thereof.
[3] DGB/2021/12 or the latest iteration thereof.
[4] DGB/2021/11 or the latest iteration thereof.
[5] DGB/2017/09 or the latest iteration thereof.
[6] DGB/2021/17 or the latest iteration thereof.
[7] Dated 20 December 2011 or the latest iteration thereof.

## XII. Relationship with Other Issuances

49. This Policy may be complemented by administrative instructions and/or operational guidelines or manuals, as required.

50. Subject to the provisions of paragraph 51 below, this Policy complements other administrative issuances relating to data or information, such as the UNIDO Information and Communications Technology Policy,[5] the UNIDO Information Disclosure Policy,[6] and the UNIDO records retention schedule.[7]

51. Other administrative issuances shall be interpreted and applied so as to give effect to the principles of personal data protection and the rights of data subjects as set out in this Policy.

52. This Policy will be reviewed when required and normally every two years.