IDLO PERSONAL DATA PROTECTION POLICY

EFFECTIVE AS OF 10 SEPTEMBER 2018 BY ADMIN NOTICE NO.9/2018
AS AMENDED ON 5 MARCH 2021 BY ADMIN NOTICE NO. 1/2021

Table of Contents

1. Overview

In pursuit of its mission and to perform its mandate, IDLO processes personal data. Given the increasing relevance in the international and European legal context of enhancing protections for such data, this Policy provides a regulatory framework for IDLO on the processing of personal data consistent with the best standards of protection recognized by International Organizations. IDLO is committed to applying appropriate safeguards for the handling and processing of personal data as set forth in this Policy. As an intergovernmental organization, IDLO is not subject to any regional or national laws concerning data protection.

2. Purpose and Scope

The purpose of the IDLO Personal Data Protection Policy (the "Policy") is to set out principles and procedures for the processing of personal data collected, stored, and transferred by IDLO.

To carry out its mandate, IDLO collects, stores, and transfers data. While the substantial majority of the data processed by the Organization is public data and can be disclosed to the public, some of the data is personal and requires adequate protection.

The Policy sets out the principles governing the processing of personal data by IDLO and provides all IDLO personnel with a comprehensive procedure on how to manage personal data so that the right to privacy of individuals who have provided their personal data to IDLO enjoys appropriate protection. Moreover, the Policy aims to outline the rights of Data Subjects with respect to the processing of their personal data by IDLO.

The Policy applies to any processing of personal data belonging to Data Subjects for the purpose of fulfilling IDLO's mandate. Data Subjects, as defined below, can be internal and external to IDLO.

Nothing contained in the Policy shall be deemed a waiver, expressed or implied, of any privilege or immunity that IDLO enjoys as an international organization, including with respect to its employees and the inviolability of IDLO property, archives, and communications.

3. Definitions

Personal data: information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a signature, 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.

Special categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data, and data concerning health or a natural person's sex life or sexual orientation.

Biometric data: any personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person that allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Genetic data: any personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question.

Data concerning health: any personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.

Consent: any freely given, specific, and informed indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of his or her personal data.

Controller: IDLO, which alone or jointly with others determines the purposes and means of the processing of personal data.

Processor: natural or legal person, public authority, agency or other body that processes personal data on behalf of IDLO.

Data Subject: any identified or identifiable natural person. It may include, for example, individuals under a special service contract, independent consultants, interns and volunteers, applicants who applied for an IDLO position, employees of other contracting parties such as an audit firm or a service provider, or officials of stakeholders such as program partners and donors, among others.

Recipient: any natural or legal person, public authority, agency, or another body to which personal data is disclosed.

Third party: any natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor, and persons who, under the direct authority of the Controller or Processor, are authorized to process personal data.

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

Data retention: the storage of any personal data, after its collection, through secure means and for the maximum period allowed in compliance with this Policy and IDLO Document Retention Policy.

Pseudonymization: the processing of personal data in such a manner that the 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 is not attributed to an identified or identifiable natural person.

4. Principles

IDLO's processing of personal data is carried out in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.

4.1 Lawfulness, fairness, and transparency

Processing of personal data is lawful, fair, and transparent.

Processing is lawful when any of the below conditions apply:

(i) The Data Subject has given consent to the processing of his or her personal data for one or more specific purposes;
(ii) It is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
(iii) It is necessary in order to protect the vital interests of the Data Subject or of another natural person;
(iv) It is necessary to enable IDLO to carry out its mandate;
(v) It is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data;
(vi) It is necessary for the compliance with a legal obligation; or
(vii) If, when data are processed for a purpose different from the one about which the Data Subject was informed, the new purpose is compatible with the one for which the data was collected, pursuant to provision 4.2 of the Policy.

Processing of special categories of data is lawful when any of the below conditions apply:

(i) The Data Subject has given explicit consent to the processing for one or more specified purposes;
(ii) It is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security;
(iii) It is necessary to protect the vital interests of the Data Subject or of another natural person;
(iv) It relates to personal data which are manifestly made public by the Data Subject;
(v) It is necessary for the establishment, exercise, or defense of legal claims;
(vi) It is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an Employee, or for the provision of health or social care; or
(vii) It is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes and it is carried out in compliance with the principle of data minimization.

4.2 Purpose limitation

Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Prior to or when collecting data, IDLO should identify the purpose(s) for which it intends to process the data and provide an explanation. Purposes should be explained in an intelligible way in order to ensure that they are sufficiently clear to the Data Subject. The explanation should enable the Data Subject to understand what kind of processing is included within the specified purpose. Multiple related purposes may be considered to be sufficiently specified under a general descriptor, while unrelated purposes should be separately listed and explained in sufficient detail.

Further purposes are considered compatible with the original ones if, considering the link between the two purposes, the context in which the personal data was collected, and the nature of personal data:

(i) they were already implicitly or explicitly covered under the original purposes; or

(ii) the Data Subject could reasonably expect processing for such purposes.

If the new purpose is incompatible with that originally envisioned, the Data Subject should be informed about the new purpose, unless the Data Subject already has that information. If the processing was based on consent, in addition to providing information of the new purpose, a new consent should be obtained.

Further processing is always allowed and considered compatible if it is carried out for archiving purposes in the public interest or for scientific or historical research or statistical or similar purposes.

4.3 Data minimization

The processing of personal data should be limited to what is necessary in relation to the processing purposes.

Excessive personal data should not be collected. Collected data should be processed in a manner that minimizes the use of personal data that is not necessary to fulfil the purpose.

4.4 Accuracy

Personal data should be accurate and, where necessary, kept up to date.

Reasonable steps should be taken to ensure that personal data that is inaccurate is erased or corrected without undue delay.

4.5 Storage limitation

Personal data should be stored in a manner that allows identification of Data Subjects for no longer than necessary for the purposes of the processing.

4.6 Integrity and confidentiality

Personal data should be processed in a manner that ensures adequate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, by using appropriate physical, organizational, and technological security measures.

4.7 Accountability

In the event of a personal data breach, IDLO will take reasonable steps to inform the Data Subject(s) affected by the breach and will take adequate measures to promptly contain and limit the breach, as necessary and feasible, and to learn from the experience in order to prevent similar future breaches. Information and questions regarding personal data breaches will be communicated from the dedicated e-mail address (dataprotection@idlo.int).

5. Rights of the Data Subject

5.1 Right to information

When personal data is collected, the Data Subject should be provided with as much of the following information as feasible and/or applicable:

(i) The contact detail of IDLO (dataprotection@idlo.int);
(ii) The lawful basis for the processing pursuant to section 4.1 of the Policy;
(iii) The purposes of the processing;

(iv) The recipients or categories of recipients of the personal data, including any transfer to third parties outside IDLO, if any;
(v) The anticipated period for which the personal data will be retained or the criteria used to determine that period;
(vi) The Data Subject's rights and recourse pursuant to this Policy; and
(vii) The Data Subject's duty to communicate to IDLO any update of the personal data.

Any information provided to the Data Subject on the processing of their personal data should be given in simple and clear language. It should be as comprehensive as possible in relation to the reasons above mentioned and the ways in which personal data will be processed.

5.2 Right of access and data portability

The Data Subject has the right to obtain from the Controller access to personal data and, upon his or her request, information on how the personal data has been or is being processed, subject to the limitations set forth under section 6.8 of the Policy.

When exercising the right of access, the Data Subject has the right to request and obtain a copy of the personal data concerning him or her in commonly used and machine-readable format and to transmit that data to another Controller.

A data subject's right to access does not entitle the data subject to confidential information, including related to other individuals. Where necessary, a document may be redacted to provide only the personal data of the requesting individual.

5.3 Right to rectification and erasure

The Data Subject has the right to obtain from the Controller without undue delay the correction of inaccurate personal data concerning him or her. This includes the right of the Data Subject to request the completion of incomplete personal data by providing a supplementary statement.

The Data Subject has the right to obtain from the Controller the erasure of personal data concerning him or her, if:

(i) The personal data is no longer necessary for the purposes for which it was originally collected and processed;
(ii) The Data Subject withdraws the consent originally provided, in accordance with section 5.4 of this Policy, and there is no other legal ground for continuing to process the information; or
(iii) The personal data has been unlawfully processed.

IDLO may refuse to erase or to suspend the processing of personal data in case the satisfaction of such request would severely harm the operational needs and priorities of IDLO in pursuing its mandate.

5.4 Right to withdraw consent

The Data Subject has the right to withdraw his or her consent for the processing of his or her personal data. Where the withdrawal of such consent is in the context of an internal or external dispute resolution or disciplinary process involving the individual, the processing will continue for such purposes even if consent has been withdrawn.

The withdrawal of consent could lead to reversal of actions taken by IDLO in reliance on such consent, at the risk of the Data Subject. The withdrawal of consent does not preclude the processing of the same personal data for other purposes under other lawful bases.

5.5 Right to object

The Data Subject has the right to object at any time to the processing of his or her personal data on the basis of compelling legitimate grounds as determined by IDLO.

IDLO will accept the objection if it determines that the fundamental rights and freedom of the Data Subject in question outweigh IDLO's legitimate interest, or the public interest, in continuing the processing.

6. Personal Data Processing

6.1 Collecting personal data

Prior to or when IDLO collects for processing personal data from an individual, it will provide the Data Subject with information as provided under section 5.1 of this Policy.

6.2 Obtaining informed consent

When personal data is collected and processed on the basis of consent, pursuant to section 4.1(i), such consent may be obtained in a variety of forms, including orally, though written consent is always preferred. Consent may be obtained electronically, including through the process of accessing the IDLO website or submitting various forms or information to IDLO. When consent is provided orally, written consent should be provided thereafter with an indication that consent has been already obtained orally.

Written consent forms or records should be processed by the Office that collected them. The Human Resources and Office Services (HROS) Department may access written consent forms or records upon request.

6.3 Duty of the Controller and Processor during the processing

In processing personal data, the Controller, the Processor, and their staff should implement appropriate technical and organizational measures to ensure that processing is performed in accordance with the principles, Data Subject rights, and operational rules set forth in this Policy and will be responsible for rectifying any breach in the confidentiality and security of personal data. IDLO includes in its General Terms and Conditions of Contract provisions aimed at ensuring the confidentiality of the personal data processed on its behalf by processors.

While IDLO does not generally carry out activities which are likely to result in a high risk to the rights and freedoms of natural persons, in those cases where a new operation is likely to result in such risk, IDLO will endeavor to carry out an assessment of the impact of the processing operations on the protection of personal data.

6.4 Record of processing

IDLO will endeavor where feasible to maintain a record of its processing activities.

6.5 Confidentiality and security of personal data

Pursuant to the IDLO Document Retention Policy, data can be considered as Confidential, Private, or Public. Personal data will usually be treated as Confidential and protected as such. This includes limiting access to personal data, to the extent feasible, only to those who need to use it. Nevertheless, some personal data which are not of a sensitive nature may not be considered confidential and may be shared with IDLO users or authorized external partners on the internal network.

All employees of IDLO are responsible for ensuring that any personal data that they hold is kept securely consistent with this Policy and not disclosed without any needed authorization. IDLO will implement appropriate organizational and technical measures to help ensure a high level of data security proportionate to the risks related to the nature and processing of personal data and the feasibility and cost of such measures. Such measures include setting up any necessary procedures for handling particular types of data in the relevant departments and offices, organizing Employee training on data protection, and maintaining adequate security of IDLO premises, files, and ICT systems.

6.6 Retention of personal data

Personal data will be retained in accordance with the IDLO Document Retention Policy. Personal data contained in documents which are subject to long retention periods may be pseudonymized or redacted if they are not necessary for the understanding of the document content.

Personal data may be stored without needing pseudonymization or redaction if the personal data will be processed solely for archiving purposes in the public interest or for scientific or historical research or statistical or similar purposes.

The original or electronic copy of the document should always remain within IDLO's premises and, in case of a request to access to personal data, only a copy of it should be provided.

Personal data will be disposed of in a way that protects the rights and privacy of Data Subjects. Depending upon the sensitivity of the data, this may include shredding and deletion from ICT systems and backups or, in case of recovery processes, the data will be excluded from the restoring procedure.

6.7 Transfer of personal data to third parties

IDLO may need to disclose personal data to third parties in order to fulfil its mission requirements.

If the Data Subject was not previously informed of the possibility of his or her personal data being transferred to third parties, the Data Subject should be informed of the disclosure.

In the context of the transfer to a third party, IDLO will generally seek assurances from such party, for example through contractual clauses or other types of mutual arrangements, that the party will provide an adequate level of protection to the personal data transmitted by IDLO.

If such level of protection by the third party is not assured, IDLO will consider options to mitigate the risks of the transfer such as, for example, seeking the specific consent of the Data Subject to the transfer.

6.8 Request of access, data portability, correction, objection to processing, erasure of personal data and withdrawal of consent

The Data Subject may exercise his or her rights as set forth in this Policy by submitting a request to dataprotection@idlo.int. Such request will be received by the data protection focal points of the HROS Department. IDLO will process the request without undue delay and a reply to the request should be provided in writing within 1 month.

When the Data Subject exercises his or her rights provided by this Policy, the Office that processes the data, in collaboration with HROS and the Office of the General Counsel (OGC), will assess whether legitimate grounds for satisfying the request exist and, if so, advise all relevant processors to proceed accordingly.

In evaluating a response to such a request from a Data Subject, IDLO will weigh the interest of the Data Subject against the interest of the other parties concerned, including IDLO, its employees and other Data Subjects. IDLO may deny a request in whole or in part where:

(i) satisfying the request could adversely affect the rights and freedoms of others;
(ii) requests from a Data Subject are manifestly unfounded or excessive, for example because of their repetitive character;
(iii) IDLO is not in a position to identify the Data Subject;
(iv) it is necessary to safeguard or ensure IDLO's overriding operational needs and priorities;
(v) it is necessary for IDLO to exercise or defend legal claims of any nature (including in internal dispute resolution mechanisms or arbitration); or
(vi) it is necessary to protect the rights of another natural or legal person.

7. Competent authority and enforcement

7.1 Authority

Each IDLO Department and Country Office is responsible for ensuring that its processing of personal data is carried out pursuant to the Policy and that its operations are carried out with due consideration for protection of processed personal data. For this purpose, each Department and/or Unit, as determined by the Director, will appoint a focal point for data protection.

The Office of the General Counsel is the responsible office for providing advice on the interpretation or application of the Policy and addressing issues that may arise relating to compliance with the Policy and the processing of personal data. Anyone needing clarification on the meaning of or compliance with the Policy may seek advice from OGC.

The Human Resources and Office Services Department is the receiver of data subject requests and is responsible for consulting OGC and the focal point of the Department and/or Unit that collected the personal data to address such requests. HROS also notifies Data Subjects of data breaches that may have occurred in relation to their data.

The Director-General is the competent authority for taking any final decision on data protection-related matters or disputes.

7.2 Breach of the Policy and dispute resolution

Any detected breach in the confidentiality or security of personal data must be notified to HROS without undue delay. HROS will coordinate with relevant Departments and OGC on the adoption of reasonable measures necessary to:

(i) remedy such breach or protect the personal data against any breach or threat; and

(ii) prevent an equivalent breach in the future.

Any Data Subject employed by IDLO (or otherwise covered by its regulations and rules) who believes that his or her right to data protection under this Policy has been infringed by IDLO may pursue redress through the informal and formal dispute resolution procedures set forth under Chapter 11 of IDLO's Employee Regulations and Rules.

Any Data Subject not employed by IDLO or subject to its regulations and rules who believes that his or her right to data protection under this Policy has been infringed by IDLO may pursue redress by directing the concern to the dedicated data protection e-mail address: dataprotection@idlo.int.

If they are dissatisfied with the determination they may request a review of that decision by the Director-General of IDLO. The decision of the Director-General is final and is not subject to review, challenge, or other action or process before any other forum.

7.3 Privileges and Immunities

The Policy provides a comprehensive regulation of personal data protection in accordance with the scope defined above and is in lieu of any national or regional law on personal data protection. IDLO as an intergovernmental organization is not subject to any national or regional law on data protection and nothing in this Policy is intended to derogate from any of the Privileges and Immunities that IDLO enjoys as an International Organization.