IDLO PERSONAL DATA PROTECTION POLICY

EFFECTIVE AS OF 10 SEPTEMBER 2018 BY ADMIN NOTICE NO.9/2018

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 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 provides all IDLO employees, and, employment candidates, and, other data subjects who have provided their personal data at the request of IDLO with a comprehensive procedure on personal data protection so that an individual's right to privacy enjoys appropriate protection. Moreover, the Policy aims to provide Data Subjects with rights 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 hereinafter, can be internal and external to IDLO.

Nothing contained in the Policy shall be deemed a waiver, express 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 archives and communications.

3. Definitions

Personal data: any 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, genetic data, biometric data, 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, which 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 which give unique information about the physiology or the health of that natural person and which 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/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 which 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, other contracting parties such as an audit firm or a service provider, or stakeholders such as program partners and donors, among others.

Recipient: any natural or legal person, public authority, agency or another body, to which the 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, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data transfer: Any transfer of data to other International Organizations or third parties taking place in the context of an agreement between IDLO and Implementing Partners or Donors or other third parties.

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 shall be carried out in compliance with the principles of lawful, fair and transparent processing, 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 its consent to the processing of his/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 for which the Data Subject has given consent, 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 where the Data Subject is physically or legally incapable of giving consent;
(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 the Employee, 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.

Any information provided to the Data Subject on the processing of its personal data should be given in a transparent manner, which means in a concise and intelligible way and by using 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.

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 for which it intends to process the data and provide an explanation of it. 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 and to assess the consistency of the processing with the stated purposes. 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 for which consent was obtained, the Data Subject should be informed about the new purpose and a new consent should be obtained.

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

Every reasonable step 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.

If, pursuant to the IDLO Document Retention Policy, the document in which the personal data is contained is retained for a longer period than that necessary for the processing of data, the personal data that is no longer needed should be pseudonymized or redacted.

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, historical research, statistical or similar purposes.

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 data breach, IDLO 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. In the event of a data breach, the Data Subject may exercise his or her rights pursuant to Article 7.2 of this Policy.

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 before he/she gives consent:

(i) The identity and the contact detail of the Controller;
(ii) The purposes of the processing;
(iii) The recipients or categories of recipients of the personal data, if any;
(iv) Whether the Controller intends to transfer the personal data to a third party outside IDLO;
(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;
(vii) Whether the provision of personal data is required by IDLO's regulations, rules or employment handbook, or is a contractual requirement;
(viii) The Data Subject's duty to communicate to IDLO any update of the personal data; and
(ix) Whether the personal data may be disclosed to third parties for processing purposes.

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/her request, information on how the personal data has been or is being processed.

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 without hindrance from IDLO.

However, IDLO will not distribute to third parties any document containing IDLO information, aside from the Data Subject's personal data that is classified as private or confidential under IDLO's Document Retention Policy. In relation to documents classified as private or confidential, IDLO may at its discretion circulate the document to a third party with Data Subject consent.

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;
(iii) The Data Subject objects to the processing in accordance with section 5.5 of this Policy;
(iv) The personal data have 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 except where the withdrawal of such consent is in the context of an internal or external dispute resolution or disciplinary process involving the individual and IDLO or will cause harm to IDLO as determined by the Director-General.

5.5 Right to object

The Data Subject has the right to object at any time 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 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 Obtaining informed consent

Prior to or when collecting the personal data, IDLO should provide the Data Subject with the information enlisted under article 5.1 of this Policy. If special categories of data are collected, specific consent for this category of data should also be obtained.

Consent may be obtained in a variety of forms, including orally, though written consent is always preferred. Consent may also 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 of the date in which the consent has been obtained orally.

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

If personal data that has already been collected requires further processing for another purpose, the Controller will provide the Data Subject with information on how the data will be furtherly processed.

6.2 Duty of the Controller and Processor during the processing

In processing personal data, the Controller, the Processor and their staff shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate 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 that is outside the responsibility of ICT. They will seek advice from the Office of the General Counsel (OGC) in case of doubt on the correct way to process data pursuant to the Policy.

6.3 Record of processing

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

6.4 Confidentiality and security of personal data

Pursuant to the IDLO Document Retention Policy[1], data shall be considered as Strictly Confidential, Confidential, Private or Public. Personal data will usually be treated as Private and protected as such. This includes limiting access to personal data, to the extent feasible, only to those who need to use it.

All Employees are responsible for ensuring that any personal data which they hold is kept securely consistent with this Policy and is 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.

6.5 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 if they are not necessary for the understanding of the document content.

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.

6.6 Transfer of personal data to third parties

IDLO may need to disclose personal data to third parties in order to fulfil its mission requirements. In such event, IDLO should obtain the consent of the Data Subject to such disclosure whenever feasible after having informed him or her that the Third Parties to which the data is being disclosed may not guarantee the same level of protection.

6.7 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 the Office that collected them. The recipient Office, in collaboration with HROS will process this request. Action on the request should be taken without unduly delay and a reply to the request should be provided in writing within 1 month.

[1] Any relevant IDLO Policy on Document Retention

When the Data Subject exercises his or her rights provided by this Policy, the Office that collected the data, in collaboration with HROS and OGC will assess whether legitimate grounds for satisfying the request exist and, if so, advise all relevant processors to proceed accordingly. In case of request for data access or portability, the Office that collected the data should provide the Data Subject with the requested information at the earliest opportunity.

7. Competent authority and enforcement

7.1 Authority

OGC is the responsible office for providing advice on the interpretation or application of the Policy and for addressing issues that may arise relating to compliance with the Policy and the processing of Personal 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 the personal data must be notified to HROS without undue delay, which will coordinate with relevant Departments and OGC on the adoption of all 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 their concern to the IDLO Office of the General Counsel. If they are dissatisfied with the determination of the General Counsel 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.