

UNICEF POLICY ON PERSONAL DATA PROTECTION

Document Number: POLICY/DFAM/2020/001

Effective Date: 15 July 2020

RATIONALE

1. UNICEF uses personal data in a range of activities, whether it is to carry out beneficiaries' needs assessments, to implement child protection programmes, to tailor supporters' engagement or to manage human and supply resources. Examples of personal data include data that directly identify an individual (e.g. a name, a date of birth) or combinations of data (e.g. demographic data, location data) that make the individual identifiable. What constitutes personal data is dynamic and contextual. A single data source may not make an individual identifiable. However, in combination, and with the application of new technologies, data sources may make the individual identifiable. Therefore each data source should be assessed for actual or potential personal data content.
2. UNICEF must consider opportunities and risks in the use of personal data, including in combination with evolving technologies (e.g. biometrics, artificial intelligence). The protection of this data is essential to upholding fundamental rights to privacy¹ and the UN-system wide personal data protection and privacy principles. This Policy implements these UN principles and governs the processing of personal data by UNICEF. The Policy stipulates a compliance framework for appropriate personal data protection throughout the data life cycle (e.g. collection, storage, analysis, transfer, deletion, or collectively, 'processing'). Under the Policy UNICEF commits to process personal data in ways that are appropriately: i) justified; ii) for defined purposes; iii) limited in scope to that necessary for defined purposes; iv) performed for accuracy and currency; v) secure and confidential; vi) limited in time; vii) transparent to the persons the data is about, and allows requests for access, change, deletion, or limits on processing (including automated decision-making); and viii) protected upon transfer to others. Related implementation measures are provided.
3. This Policy is without prejudice to the 1946 Convention on the Privileges and Immunities of the United Nations.

SCOPE OF APPLICATION

4. This Policy uses terms, such as "personal data", "data subjects", "processing", "data controller" and "data processor" and other terms as defined in Annex 1.
5. This Policy applies solely to the processing of the personal data of living individuals.
6. This Policy applies only to personal data collected and/or further processed by UNICEF filing systems, and provides protection that is appropriate to the risks and sensitivity regarding the personal data processed by particular filing systems.
7. All UNICEF personnel are required to process personal data in accordance with this Policy. Roles and Responsibilities are identified in Annex 3.

¹ Including in the Universal Declaration on Human Rights, article 12 and the Convention on the Rights of the Child, Article 16.

8. The following topics are outside the scope of this Policy: (a) anonymous or anonymized information processed for statistical and research purposes; (b) data that can identify a group, demographic or community, but *not* an individual; (c) personal data of deceased data subjects; and (d) confidential information that does not include personal data.² These matters may be subject to possible regulation under other Policies, or warrant application of principles from this Policy, *mutatis mutandis*.
9. This Policy complements other UNICEF regulations relating data or information, such as the Information Disclosure Policy and the Procedure on Information Management. This Policy shall be implemented subject to: i) overriding legal obligations, such as relevant resolutions, regulations, rules or decisions of the General Assembly, Secretary General or Executive Board; ii) the Office of Internal Audit and Investigation Charter and iii) fundamental rights and freedoms of the data subjects or other persons.

POLICY STATEMENTS

10. In its interpretation and application to the personal data of a child, the best interest of the child shall be a primary consideration, and an interpretation and application that does no harm shall be sought.
11. UNICEF personnel shall take particular care in processing the personal data of children and vulnerable categories of data subjects.
12. The processing of particularly sensitive personal data is allowed only where necessary to carry out UNICEF's mandate. Where such processing occurs, appropriate organizational and technical safeguards shall be used to protect the data subjects against identified risks associated with the processing, including the risk of discrimination.
13. The respective roles and responsibilities (as a controller or a processor) of UNICEF and UNICEF associates must be defined prior to the collection and further processing of personal data to ensure accountability under this Policy.
 - 13.1. As a controller, UNICEF may only engage with processors, including UNICEF associates, that provide appropriate commitment and assurance of meeting the requirements of this Policy or equivalent personal data protection standards, with the exception of paragraphs 43 to 49. As a joint controller, UNICEF shall agree in writing with other controllers the responsibilities of each and shall disclose the arrangement to the data subject where appropriate.
 - 13.2. As a processor, UNICEF will notify data controllers of its data protection requirements and will not knowingly process personal data received that were not collected in compliance with this Policy. UNICEF may only process data on documented instructions from the controller, subject to any pre-existing obligations UNICEF has to process that were disclosed to the controller. UNICEF may only engage with (sub-)processors, including UNICEF associates, upon consent of the controller, and where the (sub-)processor agrees to assume the same data protection obligations as UNICEF made to the controller.
14. Risks associated with the processing of personal data shall be managed in accordance with UNICEF's Enterprise Risk Management Policy, including by taking into account the confidentiality and level of sensitivity of the personal data that are processed.

² Such as business secrets: see UNICEF Information Disclosure Policy.

Policy Elements

Personal data protection principles

Legitimate and fair processing

15. One or more legitimate bases is required for the processing of personal data. The legitimate bases are:
 - (i) the consent of the data subject, or the child's representative where appropriate ("consent");
 - (ii) to prepare for or perform a contract with the data subject, including a contract of employment ("contract");
 - (iii) to protect the life, physical or mental integrity of the data subject or another person ("vital interests");
 - (iv) to protect or advance the interests of people UNICEF serves, and particularly those interests UNICEF is mandated to protect or advance (this legitimate basis would constitute "UNICEF's legitimate interest" as well as the "beneficiary interest");
 - (v) compliance with a public legal obligation to which UNICEF is subject ("legal obligation");
 - (vi) other legitimate interests of UNICEF consistent with its mandate, including the establishment, exercise or defense of legal claims or for UNICEF accountability ("other legitimate interests").
16. Consent, often supported by other legitimate bases, is the preferred basis for processing. In some cases, obtaining consent may be impractical, including because: the data subject is an under-13 child or a child whose age cannot be determined, and consent cannot be sought from a child's representative; the capacity of the data subject to consent cannot be reasonably assessed, and substitute alternative consent is unavailable; or there is urgency and the timely grant of consent by the data subject is not expected.
17. Personal data shall be processed in a manner that is transparent to the data subject, in conformity with paragraphs 25 and 26.

Purpose specification

18. Personal data shall be processed for specified and limited purposes, which are consistent with the mandate of UNICEF and are determined prior to the time of collection.
19. UNICEF may further process personal data for purposes other than those specified at the time of collection: i) if consent is obtained to further processing; ii) if such further processing is compatible with those original purposes and the risks of further processing do not outweigh the benefits it entails for the data subject; iii) if UNICEF is required to process further for statistical, historical or scientific purposes; iv) to establish UNICEF accountability; or v) for the establishment, exercise or defense of legal claims.

Necessity and proportionality

20. The processing of personal data shall be relevant, limited and adequate to what is necessary in relation to the purpose(s) specified for processing. This requires, in particular, ensuring that the personal data collected are not excessive for the purposes for which they are collected, and that the period for which the data are stored in the UNICEF filing system, is no longer than necessary, in conformity with paragraph 24.

Accuracy

21. Reasonable efforts shall be made to process personal data with accuracy and currency. The accuracy of the personal data to be retained shall be reassessed periodically. Frequency of accuracy review will depend on factors such as the relative time sensitivity of the personal data. Determination of reassessment frequency shall be substantiated and documented. Personal data in archives need not be reassessed, corrected or kept current.

Security

22. Personal data shall be classified in accordance with a contextual assessment of its sensitivity, in accordance with UNICEF information security standards.
23. Appropriate organizational, administrative, physical and technical safeguards and procedures shall be implemented to protect the security of personal data, including against or from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability. Such measures may include logging access, changes to or deletion of personal data.

Limited retention

24. Personal data shall be retained in the UNICEF filing system:
 - 24.1. Permanently, if and only if the criteria under UNICEF's policies and procedures on archiving are met;
 - 24.2. For the time required to achieve the purposes for which the personal data were collected. Those responsible for stipulating and implementing appropriate retention standards shall substantiate and document i) how long the personal data is needed for the intended purpose(s), ii) after which period of time the data will become stale or no longer useful for the intended purpose(s), iii) the appropriate retention period for the personal data based on assessment of retention needs, iv) how to safely and appropriately destroy or archive the personal data at the end of the determined retention period. Note: retention periods exceeding 10 years require additional substantiation.

Notice of personal data processing

25. UNICEF shall provide to the data subject the information contained in Annex 2, when collecting their personal data.
26. When personal data are collected by UNICEF (as controller) from a source other than the data subject or child's representative, the information contained in Annex 2 shall be provided to each identified data subject within a reasonable period, having regard to the logistical constraints to which UNICEF is subject.

Data subject requests to interact with their personal data

27. Access, correction, deletion, objection and restriction to processing of personal data, and objection to automated decision-making may be requested, subject to the conditions below, by an individual who provides sufficient evidence of being the relevant data subject or associated child representative.
28. Such requests shall be limited to personal data within UNICEF's filing system that directly identify the data subject and not to data that could indirectly identify the data subject.
29. Where such requests relate to personal data held in unstructured format, including written reports, and other files from which personal data extraction would not be possible employing reasonably available resources, UNICEF would generally decline to fulfill the request, unless overriding considerations demanded otherwise. Such overriding considerations could include upholding the best interest of the child or fundamental rights and freedoms of individuals.
30. Data subject requests shall be addressed by UNICEF in accordance with the mechanism set out in Annex 2, taking into account possible overriding considerations in the application of this Policy (see paragraph 9) and the provisions below.

Access

31. Unless it adversely affects the rights and freedoms of others, upon request, the data subjects or child's representatives shall be provided with confirmation as to whether personal data concerning the data subject are being processed, and, where that is the case, information about requested categories of personal data held by UNICEF.
32. Access to UNICEF archives shall be provided in accordance with applicable policies and procedures specific to archives.

Correction

33. A request from the data subject or associated child's representative to update or correct personal data shall be granted, unless the requested change would be inaccurate or the data are contained in a record held in the UNICEF archives.
34. In order to preserve the integrity of UNICEF archives, a note may be included in the relevant archival file to indicate that a correction request has been made.

Deletion

35. Subject to paragraph 36, a request by a data subject or child's representative to have personal data deleted from the UNICEF filing system shall be granted when: i) the personal data were not processed in compliance with this Policy; ii) retention of the personal data would not be in compliance with this Policy; iii) in cases where the only legitimate basis for processing is consent, the data subject withdraws the consent on which the processing was based; or iv) a request has been granted to fully restrict processing under paragraph 38.
36. Personal data shall not be deleted in the following circumstances: i) there are overriding vital interests, beneficiary interests, legal obligations or other legitimate interests; ii) UNICEF is required to process further for statistical, historical or scientific purposes.
37. Records held in UNICEF archives shall not be deleted, in order to preserve the integrity of UNICEF records.

Objection to and restriction of processing

38. Data subjects or the relevant child's representatives may, at any time, object to or request restriction of the processing of their personal data if: i) the processing would not be in compliance with this Policy; ii) in cases where the only legitimate basis for processing is consent, the data subject withdraws the consent on which the processing is based; or iii) on compelling grounds relating to their particular situation. The request shall be granted unless there are overriding vital interests, beneficiary interests, legal obligations or other legitimate interests.

Automated decision-making

39. Data subjects shall be entitled not to be subject to a decision based solely on automated processing, which produces adverse legal or significant material 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 UNICEF, or is necessary for beneficiary interests or other legitimate interests (and provided that appropriate safeguards are in place).

Personal data transfers

40. Transfers may only occur when there is a legitimate basis for both personal data transfer and data processing. What constitutes a legitimate basis has been set out in paragraph 15 above, and these legitimate bases apply equally to data processing and data transfers.
41. Each of the data protection principles and sections of this Policy applies equally to data processing and data transfers. In particular, transfers shall only occur where the conditions set out in paragraph 13 are met.

Policy Implementation

Awareness-raising

42. UNICEF shall provide training and take appropriate action to raise awareness so as to ensure the effective implementation of this Policy by its personnel, taking into account resource and logistics constraints.

Planning

43. In acting as a controller and determining the means of processing personal data (including when creating databases), UNICEF shall incorporate “data protection by design and by default” into planning, development and decision making, and implement appropriate technical and organizational measures, such as data minimization and pseudonymization.
44. When UNICEF acts as a controller and the processing of personal data is likely to involve high risks to the rights and freedoms of the data subjects, in particular where new technologies are involved, a data protection impact assessment (DPIA) shall (and in other cases may) be conducted prior to the processing to identify the risks, any corresponding mitigating measures, and inform whether the processing shall proceed.

Monitoring

45. UNICEF shall take practical measures to monitor compliance with this Policy, including the development and maintenance of centralized registers of:
 - 45.1. Key measures taken by offices to implement this Policy;
 - 45.2. UNICEF filing systems that include personal data, which register shall contain i) the name and contact details of the information asset owner; ii) the purposes of the processing; iii) categories of the data subjects and data sources; (iv) types of personal data concerned; v) categories of recipients to whom the personal data have been or can be disclosed or otherwise transferred; vi) default retention periods; and vii) where possible, a general description of the technical and organizational security measures pursuant to 23.
 - 45.3. personal data breaches, and the nature of any data subject notifications made because of those breaches.

Personal data breach

46. A personal data breach regulation shall be established, addressing, among other things, appropriate reporting channels, review or investigations of incidents, technical responsive measures, and notifications to data subjects and others.

Accountability

47. Roles and responsibilities for implementing this Policy appear in Annex 3. A failure to comply with the Policy may amount to misconduct (particularly if the result of gross negligence, recklessness or deliberate conduct).
48. UNICEF shall define other requirements of an implementing structure, Procedures, Standards and Guidance to operationalize and monitor implementation of this Policy. UNICEF shall adopt an appropriate oversight structure to interpret the Policy, in particular, if handling data subjects' requests.

Special considerations in Emergency Contexts

49. In designated emergencies, derogation to data protection regulations may exceptionally be provided by the Director of EMOPS, after consultation with the OED/Child Safeguarding office and the UNICEF Country Representative, and in line with EMOPS and OED/Child Safeguarding guidance on data protection in humanitarian action. Derogations may address: the selection of legitimate bases for processing; assessment of necessity and proportionality in processing; accuracy, security and retention measures; the timing, format and method of notice to data subjects regarding the processing of their data; assessment of the adequacy of safeguards on transfers; the form of data protection impact assessments; and the timing of responses to data subject requests and central registration of filing systems.

Transitional Measures

50. This Policy shall be progressively implemented. There will be a 12 months transitional period from the effective date noted above for full adherence to the policy document. During this time, a comprehensive implementation plan will be rolled out. Successful completion of the implementation plan will require full cooperation at the Division, Region and Country levels regarding key implementation activities such as the compilation of personal data inventories; performance of data risk assessments; the drafting of guidance and notice documents and data protection training (e.g., train the trainer activities, etc.). Requests for implementation delay such as exemptions from specific provisions of this Policy, for specific time periods and filing systems, may be granted by the Deputy Executive Director (Management), following a request made by a Division or Regional Director, following a risk assessment. Such exemptions shall be noted in any relevant information notice.

ANNEX 1: DEFINITIONS

1. **Archives** are, as the context requires, either physical or electronic recorded information that has been deemed of sufficient administrative, fiscal, legal, historical or informational value as to warrant permanent retention under the relevant UNICEF regulation, or a designated facility containing such information objects.
2. **Anonymous or anonymized information** means information about a person whose identity cannot be determined.
3. **Child's representative** means a parent, legal guardian, or other individual legally responsible for the child in question with respect to issue being addressed.
4. **Child or children** refer to individuals who are under 18 years of age.
5. **Consent** means, in light of the information provided to the individual data subject, any freely given, specific and informed agreement of a data subject to the processing of their personal data. In the case of under-13 children, such consent shall be provided by the child's representative, with due consideration of the best interest of the under-13 child. Consent as defined and used in this Policy is intended to provide the data subject with agency as to the collection and further processing of their data. The consent is often supported by other legitimate bases for data processing such as UNICEF's legitimate interest, beneficiary interest, vital interest or contract. Data subject requests for withdrawal or alteration of consent will be reviewed and acted on with due consideration to the best interest of the child and the legitimate bases relied on for the collection and processing of the personal data.
6. **Controller** means the entity or individual, including a public authority, agency or other body, who, alone or jointly with others, determines the purposes and means of the processing of personal data.
7. **Data Protection Impact Assessment (DPIA)** means a standardized assessment building on the HLCM Principles and other recognized international data protection principles that assesses the impact of the envisaged processing activities on the protection of personal data and on the rights and freedoms of the data subjects. A DPIA aims to identify mitigating measures, if any, in order to avoid or minimize such impact.
8. **Data subject** means an individual whose personal data is subject to processing under this Policy, regardless of who provided the personal data or how it was found. For the purpose of the Policy, the term data subject includes, but it is not limited to past, potential or current beneficiaries, individual donors, supporters, suppliers, individuals in other UNICEF associate organizations and personnel.
9. **Information Asset Owner** means an individual or group designated pursuant to the *UNICEF Standard on Information Security: Asset Management*.
10. **Particularly 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.
11. **Personal data** means any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to i) an identifier such as a name, an identification number, audiovisual materials, location data, an online

identifier, ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual or iii) assessments of the status and/or specific needs, such as in the context of assistance programmes. The definition of what constitutes personal data is contextual and expanding particularly due to enhancements in technology and methods for identifying individuals.

12. **Personal data breach** means a breach of security leading to the accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability of personal data that is unencrypted or can be decrypted.
13. **Personal 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 (electronically or physically). Movement of data or provision of access to data to other individuals within UNICEF is not a personal data transfer. Personal data transfer includes transfers within a country as well as data transfers from the country where the data was originally collected to another country or countries.
14. **Process or processing** means any operation or set of operations performed on personal data, whether by automated means or manually, such as collecting, recording, structuring, consulting, retrieving, using, transferring, disclosing, sharing or otherwise making available, or deleting.
15. **Processor** means an individual or entity, including a public authority, agency or other body, which processes personal data on behalf of the controller.
16. **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.
17. **UNICEF associate** means one of the following kinds of entities with which UNICEF has a contractual relationship or collaboration arrangement: a civil society partner, bilateral or multilateral partner, National Committee, supplier or vendor, corporate partner, or a sub-contractor of any of these entities. It does not include governments.
18. **UNICEF filing system** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. This includes databases and other repositories of personal data, as well as archives, administered by or on behalf of UNICEF.
19. **UNICEF personnel** means UNICEF staff, individual consultants and contractors, UNVs, interns, volunteers, gratis personnel, UNICEF goodwill ambassadors, individuals serving on loan or deployed under Stand-by Personnel arrangements to UNICEF, and persons working for UNICEF through an employment agency or similar arrangement.
20. **Under-13 child** means a child who is below the age of 13 years as proven by any available means of identification. In the absence of such a document, the term means a child who is likely to be under the age of 13 years according to the assessment of the person collecting the personal data.

ANNEX 2: REQUESTS OF IDENTIFIED DATA SUBJECTS TO INTERACT WITH THEIR PERSONAL DATA

Provision of information about the processing of a data subject's personal data

1. Pursuant to paragraph 25 and 26, the following information shall be provided to the data subject or child's representative, in writing or orally:
 - 1.1. the purposes for which their personal data will be processed;
 - 1.2. whether personal data about the data subject will be collected from other sources, and the categories of such sources (which could include other UN agencies, government sources, UNICEF associate sources, publicly available information);
 - 1.3. the anticipated retention period;
 - 1.4. whether their personal data will be transferred to third parties, the categories of third parties to which their personal data will be transferred, and whether they may be outside the country in which the data subject is located;
 - 1.5. the importance that data subjects provide accurate and complete personal data as well as changes to their personal situation pursuant to paragraph 21 of the Policy;
 - 1.6. how to request access to their personal data, or correction or deletion of it; to object to or to restrict the processing of their personal data; and any further recourse that might be available.
2. Such information shall be provided in a clear and plain language as well as in a format adapted to the age, maturity and vulnerability of the data subjects.

How data subjects can make requests for access, correction, deletion, objection to a restriction of processing, or objections to automated decision-making

3. UNICEF shall consider a request made orally or in writing by:
 - 3.1. An adult data subject;
 - 3.2. A child data subject who is 13 or older and has apparent capacity to understand the nature and appreciate the consequences of the request, with due consideration of the best interest of the child;
 - 3.3. A child's representative for a data subject who is a child between 13 and 18, upon assent of the child and with due consideration of the best interest of the child;
 - 3.4. The child's representative for a data subject for an under-13 child, with due consideration of the best interest of the child.

UNICEF responses to requests for access, correction, deletion, objection to a restriction of processing, or objections to automated decision-making

4. In assessing or responding to the request, the person responding:
 - 4.1. May ask for further detail, if the request does not contain sufficient detail to enable UNICEF to identify and locate the record with reasonable efforts;
 - 4.2. Shall, where possible, respond to the request within a reasonable time, orally or in writing, and pursuant to paragraph 17 and paragraph 49;
 - 4.3. Shall generally limit requests to structured personal data, unless overriding reasons demands otherwise. Such overriding reasons could include upholding the best interest of the child or essential rights and freedoms of individuals;

- 4.4. Shall not reveal personal data about the data subject, unless there is sufficient proof that the person asking for the information is the data subject, or a child's representative (consideration being given to the best interest of the child);
- 4.5. May deny the request if there are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing;
- 4.6. Shall provide reasons if the request is denied, other than if it is denied on grounds that it is manifestly abusive, fraudulent or obstructive to the purpose of processing;
- 4.7. Shall provide access in a form (oral, in print, digitally, or through online access) that is reasonably practical to UNICEF and person requesting, if access is granted;
- 4.8. Shall provide information about any available recourse or review mechanism that has been established and could be used by the data subject or a child's representative.

ANNEX 3: ROLES AND RESPONSIBILITIES

Deputy Executive Director (Management)	Delegated overall responsibility for operationalization of the data protection framework within UNICEF	42-46
	Designating implementing and oversight structures to support the operationalization and interpretation of the policy	47
	Overall responsibility for making decisions associated with personal data breaches	46
Data Protection/Privacy Specialist (OED)	Providing technical advice to the Deputy Executive Director (Management), through the Senior Advisor (Child Safeguarding), in operationalizing the data protection programme within UNICEF	42-46
	Where another implementing structure has not been designated by the Deputy Executive Director (Management), providing technical assistance to offices in: effecting data protection by default and design, reviewing safeguards with associates, conducting Data Protection Impact Assessments, and addressing data subject requests	43, 13, 40-41, 44, 27-39
	Receiving, evaluating and presenting to the Deputy Executive Director (Management) annual reports on the implementation of the policy	45.1
	Advising on personal data protection aspects of personal data breaches	45.3
Regional Chiefs of Operations	Monitoring implementation of the policy in their respective regions, and through their Regional Directors, inform the Deputy Executive Director (Management) of data protection risks, and issues that impair the effectiveness of the policy or the data protection programme in general	14
Heads of Office (Regional Directors in Regions, Division Directors in Divisions, Representatives in country/area offices)	Responsible for ensuring the implementation of the policy in their offices	42-46

	Determining which and how special considerations apply to the processing of personal data during a declared emergency, across all information assets in their offices	49
	Responsible for making sure non-archival retention of records is substantiated and documented as follows:: i) how long the personal data is needed for the intended purpose(s), ii) after which period of time the data will become stale or no longer useful for the intended purpose(s), iii) the appropriate retention period for the personal data based on assessment of retention needs, iv) how to safely and appropriately destroy or archive the personal data at the end of the determined retention period. Note: retention periods exceeding 10 years require additional substantiation.	24
	Approving and signing specific agreements with associates that contain safeguards for data protection, and maintaining oversight over the implementation of the safeguards	13, 40-41
	Maintaining and keeping current a register of UNICEF filing systems that contain personal data in their respective offices	45.2
	Reporting, through the relevant Regional Chief of Operations, on the office's implementation of the policy, and designate Focal Points to assist in such reporting and coordination	45.1
	Monitoring training undertaken by the office's personnel	42
Division Directors	Responsible for prescribing appropriate general safeguards to be employed by associates whose relationship they manage, in consultation with, as appropriate, the Office of the Legal Advisor, the Data Protection/Privacy Specialist (OED) and the Chief Information Officer and his delegates	13, 40-41
	Within existing or designated regulatory authority, and as necessary, identifying, or establishing a procedure for identifying, specific data, persons or entities and activities that fall within the policy-prescribed definitions of "personal data", "particularly sensitive personal data", "controller", "processor", "processing" and "data subject"	Annex 1
	Within existing or designated regulatory authority, and as necessary, identifying, or establishing a procedure for identifying, any legal basis specified in the Policy for personal data collection and transfer, the purpose of data collection and transfer, and any exceptions based on fundamental rights and freedoms in an emergency context	Annex 1

	Within existing or designated regulatory authority, and as necessary, establishing standards and procedures for securing informed consent, and procedures to respond to requests of data subjects to interact with their personal data.	Annex 1
	Within existing or designated regulatory authority, and as necessary, establishing retention periods shorter than 10 years	24
Comptroller	Responsible for deciding whether to grant requests to retain non-archival records longer than stipulated in applicable data retention standard. And, if such request is granted, responsible for making sure exception from the applicable retention standard is substantiated and documented. Note: the granting of records retention requests where no retention standard has been promulgated, should be of temporary duration only, and contingent on prompt implementation of such retention standard.	24
Chief Information Officer and his delegates	Responsible for administration of the Information Security Programme	23
	Creating a register of personal data breaches	46
	Notifying the Information Asset Owner and/or Head of Office of a personal data breach, as part of a personal data breach response	46
Information Asset Owner (person or group designated pursuant to UNICEF STANDARD ON INFORMATION SECURITY: ASSET MANAGEMENT)	Responsible to the Head of Office in implementing and monitoring implementation of this policy in connection with a designated information asset within the UNICEF filing system	42-46

	Under the supervision of the Head of Office, and in consultation with, as appropriate, the Data Protection/Privacy Specialist (OED) and the Chief Information Officer and his delegates, determining new means of processing personal to implement 'data protection by design and by default', including by determining whether the information asset is expected to contain records of personal data	43
	Under the supervision of the Head of Office, and in consultation with, as appropriate, the Data Protection/Privacy Specialist (OED), conducting a Data Protection Impact Assessment	43
	Defining the role of UNICEF as controller or processor in connection with the designated information asset	11
	Under the supervision of the Head of Office, and in consultation with, as appropriate, the Data Protection/Privacy Specialist (OED) and the Chief Information Officer and his delegates, implementing appropriate organizational and technical safeguards in connection with the processing of particularly sensitive personal data	11
	Under the supervision of the Head of Office, determining a legitimate basis for processing data to be recorded for the designated information asset	15
	Unless otherwise prescribed by regulation, under the supervision of the Head of Office, determining how and in what circumstances consent will be pursued	16
	Specifying the purpose for personal data processing, and the personal data categories and items necessary to fulfill this purpose, based on the principle of personal data minimization.	18
	Approving further processing for purposes beyond those specified at the time of collection	19
	Documenting personal data protection measures in connection with the designated information asset	45, 50
	Periodically reassessing the accuracy of personal data. Frequency of accuracy review will depend on factors such as the relative time sensitivity of the personal data. Determination of reassessment frequency shall be	21

	substantiated and documented, and reassessment frequency should in all circumstances be less than every 5 years	
	Reviewing appropriateness of retention period and process stipulated in Retention Standard document every 5 years. Continuously ensuring that retention period and retention and destruction process stipulated in Retention Standard document are complied with.	24.2
	Under the supervision of the Head of Office, and with the advice of the Data Protection/Privacy Specialist (as appropriate) or implementing structure designated by the Deputy Executive Director (Management), receiving and deciding upon requests for access, correction, deletion, objection to and restriction of processing, or objection to automated decision-making	27-39
	Notifying affected data subjects affected by personal data breaches, as authorized under the personal data breach procedure	46
All UNICEF personnel	Knowing, understanding and applying this policy	7
	Completing prescribed courses for data protection	42
	If not already so prescribed or designated, determines whether data that they are processing constitutes personal data and communicates same to the information asset owner	4
	Determining the age of a data subject where required during personal data processing or data interaction requests, and taking particular care in the processing of personal data of vulnerable categories of data subjects	11
	Providing information about personal data processing at the time that they collect it	25-26

DOCUMENT MANAGEMENT INFORMATION PAGE

Document Title	UNICEF POLICY ON PERSONAL DATA PROTECTION
Document Number	POLICY/DFAM/2020/001
Effective Date	15 July 2020
Mandatory Review Date	15 July 2025
Responsible Business Owner	DFAM
Responsible Manager	Sigrun Kaland
Document Summary	The protection of this data is essential to upholding fundamental rights to privacy and the UN-system wide personal data protection and privacy principles. This Policy implements these UN principles and governs the processing of personal data by UNICEF. The Policy ensures that appropriate protections are applied throughout the data life cycle (e.g. collection, storage, analysis, transfer, deletion, or collectively, 'processing'). Under the Policy UNICEF commits to process personal data in ways that are appropriately: i) justified; ii) for defined purposes; iii) limited in scope to that necessary for defined purposes; iv) performed for accuracy and currency; v) secure and confidential; vi) limited in time; vii) transparent to the persons the data is about, and allows requests for access, change, deletion, or limits on processing (including automated decision-making); and viii) protected upon transfer to others. Related implementation measures are provided.
Regulatory content the Document Replaces	
Topics Covered	Requirements for the protection of personal data and the safeguarding of individuals' rights in their personal data in line with UN Data Protection Principles
Corporate Risk Area	Governance and Accountability
Reference / Links to Enabling Legislation and Background	1946 Convention on the Privileges and Immunities of the UN UN GA resolution E/CN. 4/1990/72 HLCM Principles
Links to Relevant Policy	UNICEF Information Disclosure Policy UNICEF Policy on Information Security
Links to Relevant Procedure	
Links to Relevant Guidance	
Links to Relevant Training Materials	
Links to Other Knowledge & Information Resources	