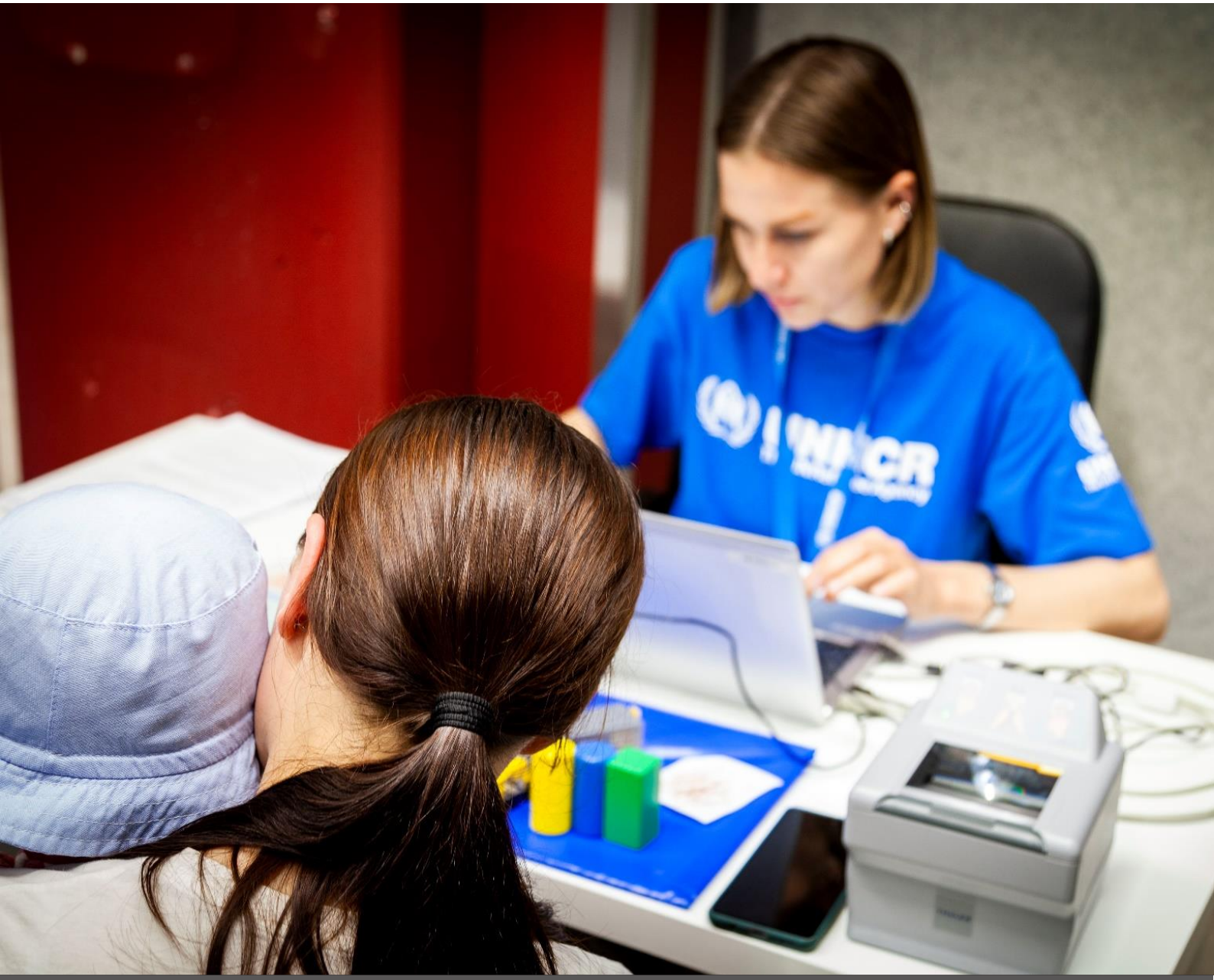
UNHCR
The UN Refugee Agency



GENERAL POLICY ON
PERSONAL DATA PROTECTION AND PRIVACY

2022

Approved by:	Filippo Grandi, United Nations High Commissioner for Refugees
Date of approval:	20 December 2022
Contact:	Chief Data Protection Officer Head of Legal Affairs Service
Date of entry into force:	31 December 2022
Review date:	By 31 December 2027

TABLE OF CONTENT

Part 1. General Provisions

(i) Purpose

1. The purpose of this General Policy on Personal Data Protection and Privacy (this Policy) is to solidify UNHCR's longstanding human rights-based approach to data protection and privacy and to set out a general framework for UNHCR to process personal data in a manner consistent with the UN Personal Data Protection and Privacy Principles, adopted by the UN High-Level Committee on Management (HLCM) on 11 October 2018.

2. This Policy establishes a unified data protection and privacy framework for the Organization, expanding beyond persons of concern and including data protection and privacy standards, the rights of data subjects, roles and responsibilities for personal data processing, and processes for the exercise of data subject rights and for complaints and redress requests by data subjects.

(ii) Scope

3. This Policy applies to the processing of personal data (including pseudonymized data). It does not apply to the processing of non-personal data (including anonymous data).

4. This Policy applies to the processing of personal data by UNHCR. It also applies to the processing of personal data on behalf of UNHCR, (for example by third parties, vendors or partners which process personal data under UNHCR's instructions) where UNHCR, alone or jointly with others, has decision-making power with respect to such processing. The Policy may apply in situations where UNHCR does not have such decision-making power.

5. Compliance with this Policy is mandatory for all UNHCR personnel.[1] Please refer to Part 5 for details on the staged entry into effect of this Policy and to paragraphs 44 through 46 for details on sharing with and processing by third parties.

6. This Policy is referred to as a "general" policy because it establishes an overall framework for the processing of personal data by UNHCR, including overarching data protection and privacy standards and principles. These standards are based upon the data protection principles set out in the Policy on the Protection of Personal Data of Persons of Concern to UNHCR.

7. With regards to the processing of personal data of persons of concern, the Policy on the Protection of Personal Data of Persons of Concern to UNHCR continues to be in effect, in line with Part 5.

(iii) Rationale

8. Data protection is the systematic application of a set of principles regarding the processing of personal data, aiming to protect the privacy of individuals and uphold their rights as data subjects. The right to privacy[2] forms an integral part of the International Bill of Human Rights.

9. In carrying out its mandate to provide protection and assistance and to seek solutions for persons of concern, UNHCR processes the personal data of various categories of data subjects. Such categories include, most importantly, persons of concern, but also extend to UNHCR personnel, donors, suppliers, partner staff, visitors and others. UNHCR is accountable for the processing of such personal data.

10. UNHCR strives towards meeting best practices in data protection when processing personal data in keeping with its role as an outward-facing, collaborative and transparent – and hence responsible and trusted – partner. UNHCR seeks to create an environment that enables the principled collection, use and sharing of personal data in furtherance of its mandate.

11. UNHCR's core activities involve providing protection and assistance to and seeking solutions for persons of concern under a mandate that is grounded in public international law, including international treaties, UN General Assembly resolutions and the good offices of the High Commissioner. The framework established by this Policy reflects a balance between UNHCR's mandate and functions and the fundamental rights and freedoms of data subjects in relation to the processing of their personal data.

(iv) Key terms

12. For the purposes of this Policy, the following definitions apply:

[1] "UNHCR personnel" means staff members and affiliate workforce. UNHCR's affiliate workforce are individuals who have a working relationship with UNHCR, including United Nations Volunteers (UNVs), individual consultants, individual contractors (including contractors under arrangements with the United Nations Office for Project Services (UNOPS) or another affiliate partner organization), fellows and deployees. UNHCR, *Administrative Instruction on Managing Affiliate Workforce,* UNHCR/AI/2020/7.

[2] See, Article 17, UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

ANONYMOUS DATA data that has undergone a technical process of removing or modifying all personal identifiers and codes in such a way that individual data subjects cannot be identified by any means reasonably likely to be used based on the data alone or in combination with other data. This is a result of a context-specific process where such technical process is complemented, as necessary, by other technical, organizational or legal measures or otherwise binding commitments to render the risks of re-identifying data subjects insignificant.

AUTOMATED DECISION-MAKING the process of making a decision through the processing of personal data by automated means and without review or intervention by an individual.

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

DATA PROTECTION AND PRIVACY IMPACT ASSESSMENT (DPIA) a tool and a process for assessing potential risks, harms and benefits to data subjects in relation to the processing of their personal data and for identifying mitigation measures, as necessary.

DATA SUBJECT an individual whose personal data is subject to processing.

PERSONAL DATA any information relating to an identified or identifiable individual.

PERSONAL DATA BREACH a breach of security leading to the accidental or illegitimate destruction, loss, alteration, disclosure of or access to personal data that is transmitted, stored or otherwise processed.

PERSONAL DATA SHARING any act of transferring, disseminating, disclosing, providing access to or otherwise making available personal data outside UNHCR.

PROCESSING OF PERSONAL DATA any operation, or set of operations (automated or not), which is performed on personal data, including collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure, access, transfer, dissemination, providing access to or otherwise making available, correction, or destruction.

PSEUDONYMIZED DATA personal data that has undergone a privacy enhancement technique where the personal data is processed 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 data security and confidentiality.

SENSITIVE PERSONAL DATA personal data which affects the data subject's most intimate sphere or relates to their immutable characteristics and which, if misused or subject to a data breach, may result in discrimination against or serious harm for the data subject, or in breaches of their fundamental rights.[3]

13. The following are terms relating to key personal data protection functions and entities in UNHCR:

PERSONAL DATA CONTROLLER the member of UNHCR personnel who has decision-making authority over the processing of personal data by country operations, regional bureaux and headquarters entities.

CHIEF DATA PROTECTION AND PRIVACY OFFICER (CHIEF DPO) the member of UNHCR personnel who independently and impartially provides expert support, advisory, monitoring and oversight functions in order to ensure UNHCR's compliance with this Policy and other policies and administrative instructions relating to UNHCR's data protection and privacy framework.

PERSONAL DATA PROTECTION REVIEW COMMITTEE a committee established to act independently and impartially to receive redress requests submitted by data subjects and perform other roles and duties allocated to it by the High Commissioner.

14. The roles, accountabilities and authorities of these functions and entities are described in Part 4 and Annex 2.

[3] This Policy does not determine a definitive list of categories of sensitive personal data. Considering the nature of UNHCR's activities and functions in furtherance of its mandate, the sensitivity of personal data may be context specific. Examples of sensitive personal data include, but are not limited to, biometrics, health data, political opinion, and personal data relating to offences, criminal proceedings and convictions. Given the particularly vulnerable position of persons of concern to UNHCR, the nature of their personal data is generally sensitive.

Part 2. UNHCR's Data Protection and Privacy Standards

15. UNHCR's data protection and privacy standards are made up of: (i) a set of data protection and privacy principles; (ii) the rights of data subjects; (iii) a set of operational standards to be applied when processing and sharing personal data; and (iv) processes when handling requests for exercise of data subject rights and complaints and redress requests submitted by data subjects.

16. These standards are minimum standards that apply to all processing of personal data by or on behalf of UNHCR, subject to permissible limitations or derogations. They may be implemented through context-specific administrative issuances and/or other UNHCR guidance documents ("implementing instruments") which concretely operationalize the data protection and privacy standards for particular UNHCR activities, operations and processes. Where appropriate, an implementing instrument may establish stricter and more protective data protection and privacy standards.

(i) Data protection and privacy principles

17. UNHCR shall process personal data in a non-discriminatory, age, gender and diversity sensitive manner, with due regard to the fundamental rights and freedoms of data subjects, including the right to privacy, and in accordance with the principles set out under paragraphs 18 through 28.

Fair and legitimate processing

18. UNHCR shall process personal data in a fair manner and only based on one or more of the following legitimate bases:

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

(b) the processing is required for the conclusion or performance of a contract with the data subject;

(c) the processing is essential for the protection of the vital interests of the data subject or another individual, or their best interests if they are a child;

(d) the processing is necessary for the performance by UNHCR of investigations or for UNHCR to establish, exercise or defend legal claims;

(e) the processing is necessary for, or otherwise enables, the performance of UNHCR's mandate or its functions:

(i) under the UN Charter, the UNHCR Statute or resolutions adopted by the General Assembly or by other organs of the United Nations;

(ii) as provided in the staff or financial regulations and rules or by any other administrative issuances adopted by UNHCR or the United Nations; or

(iii) as provided under public international law.

(f) the processing is necessary to fulfil an overriding legitimate interest of UNHCR in processing the personal data.

Purpose specification

19. UNHCR shall only process personal data for specified purposes consistent with UNHCR's mandate and functions. UNHCR shall not further process personal data in ways that are incompatible with such specified purposes.

20. Compatible purposes include processing:

(a) for the purpose of archiving personal data for its administrative, fiscal, legal, historical value;

(b) for the purpose of statistical or scientific research ;

(c) for accountability of UNHCR's actions; or

(d) when it is necessary for long-term provision of protection and assistance and seeking of solutions for persons of concern, in accordance with relevant regulations, rules, policies, administrative instructions and other instruments established or adopted by UNHCR or the United Nations.

Proportionality and necessity (data minimization)

21. UNHCR shall process personal data in a manner that is adequate, relevant and limited to what is necessary in relation to the purposes for which such personal data is being processed.

Retention limitation

22. UNHCR shall retain personal data only for the time period that is necessary for the purposes for which such personal data is being processed.

23. Personal data may be retained for a longer time period:

(a) for the purpose of archiving for its administrative, fiscal, legal, historical value;

(b) for statistical or scientific research purposes;

(c) for accountability of UNHCR's actions; or

(d) when it is necessary for long-term provision of protection and assistance and seeking of solutions for

persons of concern in accordance with relevant regulations, rules, policies, administrative instructions and other instruments established or adopted by UNHCR or the United Nations.

© UNHCR/Nicolo Filippo Rosso

Accuracy

24. UNHCR must take every reasonable step to ensure that personal data is accurate and, where necessary, kept up-to-date in such a way as to fulfil the purposes for which it is being processed.[4]

Confidentiality

25. UNHCR shall process personal data with due regard to confidentiality, in accordance with relevant regulations, rules, policies, administrative instructions and other instruments established or adopted by UNHCR or the United Nations.

Security

26. UNHCR shall apply adequate organizational, administrative, physical and technical safeguards and procedures to protect the security of personal data, including against unauthorized access and processing and against accidental loss, alteration, damage or destruction.

Transparency

27. UNHCR shall process personal data with transparency to the data subjects. This includes the provision of information, as appropriate, in a manner and language that are intelligible to the data subjects concerned, about the processing of their personal data, in accordance with paragraphs 30 and 31.

Accountability

28. UNHCR establishes accountability for compliance with this Policy through the mechanisms described in Part 4 and with the defined roles, accountabilities and authorities for implementation set out in Annex 2.

(ii) Rights of data subjects

29. A data subject has the rights set out under paragraphs 30 through 35 when UNHCR processes their personal data, including processing by a third party on behalf of UNHCR.

Information

30. A data subject has the right to information about the processing, at the time of collection of their personal data, including:

(a) the categories of personal data processed and the purposes for which they will be processed;

(b) the legitimate basis of processing, as appropriate;

(c) the anticipated retention period;

(d) where their personal data will be shared with third parties, such third parties or categories of third parties;

(e) their rights as data subjects and how to exercise them;

(f) whether processing involves automated decision-making that significantly affects them (see paragraphs 41 and 42);

(g) the contact details of the Personal Data Controller and how to access the appropriate processes for the exercise of their data subject rights and for complaints and redress requests.

31. When it is not possible to provide data subjects with all the requisite information at the first point of data collection (for example due to operational or security constraints), UNHCR must provide this information at the next practical opportunity.

Access

32. A data subject has the right to access their personal data.

Rectification

33. A data subject has the right to obtain rectification or completion of inaccurate or incomplete personal data.

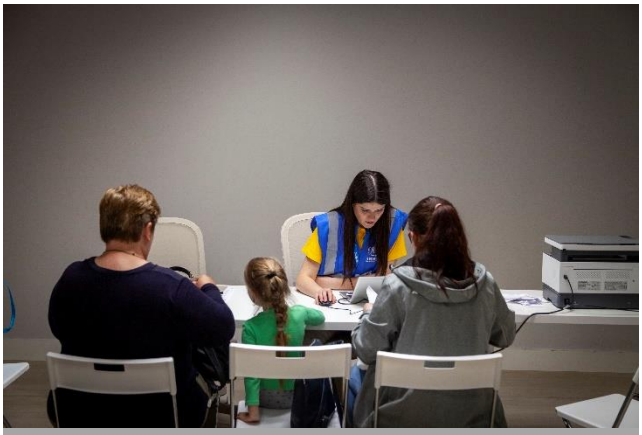
[4] The accuracy principle is without prejudice to the obligations of staff members to provide accurate personal data under the staff regulations and rules and relevant administrative issuances.

Deletion

34. A data subject has the right to have personal data deleted where there is no legitimate basis for the processing or where the personal data is no longer necessary for the specified or compatible purposes for which it was collected, unless there are grounds for retention in line with paragraphs 22 and 23.

Objection

35. A data subject has the right to object to the processing of their personal data, at any time of the processing, for legitimate grounds relating to their particular situation.



© UNHCR/Rafal Kostrzynski

(iii) Operational Standards

Data protection and privacy by design and by default

36. UNHCR shall consider data protection and privacy principles and the rights of data subjects in the development of tools, systems or processes that involve the processing of personal data or have privacy implications, from their design to their deployment, use, maintenance and ultimate disposal. UNHCR shall give due regard to available technology, resources and costs of implementation, as well as to the nature, scope, context and purpose of processing.

Data protection and privacy impact assessments

37. UNHCR shall carry out a data protection and privacy impact assessment (DPIA) for personal data processing activities that are likely to involve high risks to the fundamental rights and freedoms of data subjects, considering the nature, scope, context and purposes of the processing.

38. A DPIA is recommended for personal data processing activities that do not reach the threshold of high risk referred to in paragraph 37, but where a risk assessment or other due diligence process is appropriate, considering the nature, scope, context and purposes of the processing.

39. A DPIA will specify the anticipated risks and impact of the processing on data subjects, assess the measures for compliance with UNHCR's data protection and privacy standards, and identify mitigation measures and recommendations which will be considered and acknowledged before determining an appropriate course of action.

Personal data breach notifications

40. UNHCR shall notify data subjects as soon as possible of a personal data breach and of the measures implemented to mitigate the harm where such a personal data breach is likely to result in high risks to the security, rights and freedoms of the data subject.

Automated decision-making

41. UNHCR shall not subject data subjects to automated decision-making where a decision produces adverse legal effects or other significant adverse effects on the interests of the data subject, except where such automated decision-making is:

(a) with the consent of the data subject; or

(b) necessary for entering into or performance of a contract between the data subject and UNHCR; or

(c) explicitly authorized by a resolution adopted by the General Assembly or other organs of the United Nations or by any regulations, rules, policies or other administrative issuances adopted by UNHCR or the United Nations.

42. UNHCR shall take appropriate measures to identify and assess the potential risks, harms and benefits of automated decision-making and to prevent or mitigate any risks or harm identified for the data subjects.

Processing sensitive personal data

43. UNHCR shall apply additional safeguards for the processing of sensitive personal data, which requires enhanced data protection considering the high risk posed by its processing. Additional safeguards may include conduct of a DPIA, restrictions on processing as well as enhanced technical and organizational measures for the processing of sensitive personal data.

Sharing with and processing by third parties

44. Personal data may be shared with third parties based on arrangements that afford an adequate level of protection for the personal data, in line with the data protection and privacy principles of this Policy and with due consideration to the rights of data subjects and the

operational standards set out under paragraphs 36 through 43.

45. In addition, when a third party (a "data processor") is processing personal data on behalf of UNHCR, UNHCR will put into effect appropriate arrangements with the third party to ensure the personal data is processed only in accordance with UNHCR's instructions.

46. The arrangements referred to under paragraphs 44 and 45 may be implemented through an agreement or through other reasonable means.

(iv) Exercise of data subject rights, complaints and redress requests

47. A data subject may exercise a data subject right, make complaints with respect to UNHCR's processing of their personal data and, when not satisfied with UNHCR's response to a complaint, may seek redress, as set out in Part 2(iv).[5]

Exercise of data subject rights

48. UNHCR will grant a request by a data subject to exercise a data subject right enumerated in Part 2(ii), where the elements of the relevant data subject right are established. The Personal Data Controller will set up processes to receive, record and respond to requests by data subjects to exercise data subject rights.

49. UNHCR may refuse, in whole or in part, a request by a data subject to exercise a data subject right where:

(a) the request is manifestly unfounded, abusive, fraudulent or obstructive to the purpose of processing, or;

(b) the refusal would be a necessary and proportionate measure to safeguard:

(i) the safety and security of UNHCR, its personnel, or other individuals or groups of individuals;

(ii) confidentiality obligations of UNHCR;

(iii) the overriding operational needs and priorities of UNHCR in pursuing its mandate and functions;

(iv) the overriding rights and freedoms of data subjects, other individuals or groups of individuals; or

(c) the content, use or means of the processing of personal data falls outside the purview of UNHCR.[6]

50. A refusal of a request to exercise a data subject right will be recorded and communicated in writing to the relevant data subject.

Complaints

51. A data subject may address complaints relating to UNHCR's processing of their personal data (including complaints related to the exercise of a data subject right) to the relevant Personal Data Controller, who will review the complaint and respond to the relevant data subject.

52. When the Personal Data Controller finds that a complaint is well founded, UNHCR will take reasonable and appropriate measures and actions, in accordance with this Policy.

53. The Personal Data Controller, individually or together with other Personal Data Controllers, may establish mechanisms for receiving and responding to complaints from data subjects. The High Commissioner may also establish organization-wide mechanisms beyond those described in this Policy for receiving and responding to such complaints. Such mechanisms may be solely dedicated to data subject complaints or may be integrated into other complaint or feedback mechanisms established by UNHCR or in which UNHCR participates.

Redress Requests

54. When a data subject is not satisfied with the response to a complaint (including a failure to respond) by a Personal Data Controller, and when such complaint relates to a data subject right enumerated in Part 2(ii), the data subject may submit a redress request.

55. The Personal Data Protection Review Committee reviews whether the redress request is well founded and makes a recommendation to the High Commissioner for decision.

56. The High Commissioner decides, after consideration of the recommendation of the Personal Data Protection Review Committee, whether to grant or reject a redress request.

---

[5] The exercise of data subject rights and complaints and redress requests by staff members will be subject to additional rules and clarifications as may be set out from time to time in administrative issuances adopted by or applicable to UNHCR.

[6] For example, when the content, use or means of the processing of personal data is directly determined by the Security Council, the General Assembly, the Economic and Social Council, the International Court of Justice, or by any of their subsidiary organs, including sanctions bodies, investigative bodies, accountability mechanisms and criminal tribunals.

57. Where a redress request is granted, the remedies afforded to the data subject are limited to one or more of the following:

(a) the provision to the data subject of information in relation to a specific instance of processing of their personal data, as per paragraph 30;

(b) the provision to the data subject of a copy of the personal data being processed;

(c) the rectification of inaccurate personal data or the completion of incomplete personal data;

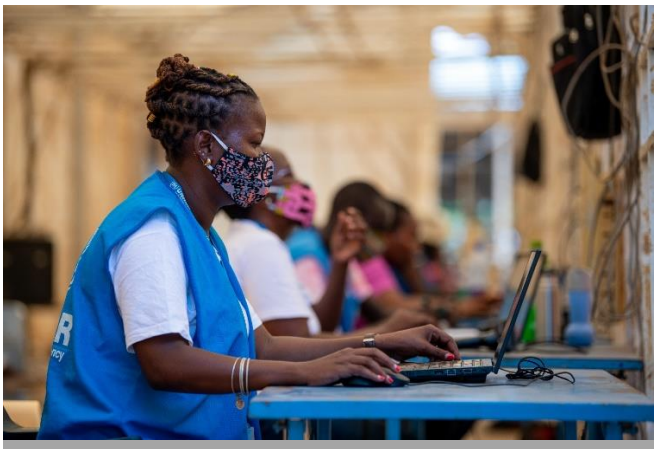
(d) the deletion of personal data;

(e) the cessation or temporary suspension of the personal data processing;

(f) a written apology to the data subject.

58. In no event will UNHCR be liable to pay financial compensation or required to make public announcements or statements.

59. The decision taken by the High Commissioner shall be communicated in writing to the relevant data subject.



© UNHCR/Samuel Otieno

60. Decisions taken by the High Commissioner on redress requests made by data subjects who are:

(a) UNHCR staff members are without prejudice to such staff member's rights regarding such decision under Article XI of the Staff Regulations and Chapter XI of the Staff Rules when such decision constitutes an administrative decision adversely affecting the rights of such UNHCR staff member and produces direct legal consequences in relation to the terms of their employment as a staff member.

(b) otherwise parties to a contractual relationship with UNHCR are without prejudice to a method of amicable resolution and dispute settlement under the relevant contract;

(c) not staff members and are not otherwise parties to a contractual relationship with UNHCR are without prejudice to any method of amicable resolution and dispute settlement set out in a separate UNHCR administrative issuance.

Privileges and Immunities

61. The processes relating to the exercise of data subject rights, complaints and redress requests referred to in Part 2(iv) are without prejudice and subject to UNHCR's privileges and immunities

Part 3. Limitations and Derogations

Limitations

62. UNHCR may establish generally applicable limitations to the rights of data subjects enumerated under Part 2(ii) or to obligations set out under UNHCR's data protection and privacy standards for one or more of the following objectives:

(a) safeguarding the safety and security of UNHCR, its personnel, other individuals or groups of individuals;

(b) investigatory and disciplinary proceedings;

(c) the overriding operational needs and priorities of UNHCR in pursuing its mandate and functions;

(d) the overriding fundamental rights and freedoms of individuals or of groups other than the data subject(s) concerned.

63. The limitation must:

(a) be issued by a member of the UNHCR Senior Executive Team or the relevant Personal Data Controller;

(b) be notified to the Chief DPO. Prior consultation with the Chief DPO is strongly recommended to ensure compliance with this Policy;

(c) be documented (for example, in an implementing instrument referred to in paragraph 16);

(d) be necessary and proportionate in relation to the objective pursued by such limitation, taking into account the nature of the personal data processed and the category of data subjects; and,

(e) not be inconsistent with the UN Charter, the UNHCR Statute, a resolution adopted by the General Assembly or by another organ of the United Nations applicable to UNHCR or with the staff or financial regulations and rules or any other administrative issuances adopted by UNHCR.

Derogations

64. The High Commissioner may authorize temporary measures relating to the processing of personal data under this Policy when it is necessary and appropriate in a declared emergency or in similar situations that are likely to interrupt the performance of UNHCR's mandate and functions, for the effective delivery of protection and assistance and to seek solutions for persons of concern or the effective performance of UNHCR activities. Where possible, such measures will be taken in consultation with the Chief DPO.

Part 4. Roles, Accountabilities and Authorities

(i) General

65. Annex 2 sets out the roles, accountabilities and authorities of UNHCR personnel in implementing this Policy.

(ii) Personal Data Controllers

66. Personal Data Controllers are accountable for compliance with this Policy with respect to the processing of the particular categories of personal data for which they have decision-making authority. The personal data processing and the accountable Personal Data Controller can be at the level of country operations, regional bureaux, headquarters or global. Their accountabilities are the same regardless of level, and include:

(a) implementation of procedures and practices to ensure and demonstrate compliance with the UNHCR data protection and privacy principles;

(b) establishment and maintenance of an inventory of the personal data being processed under their area of responsibility;

(c) coordination and consultation with the Chief DPO, as appropriate, and assistance with regard to the performance of the Chief DPO's functions.

67. Personal Data Controllers are determined as follows:

(a) The High Commissioner may designate UNHCR staff members as Personal Data Controllers with decision-making authority over the processing of personal data (including for a particular category of data subjects). In appropriate circumstances, the High Commissioner may designate two or more staff members to jointly act as Personal Data Controller.

(b) When no Personal Data Controller has been designated by the High Commissioner, the Personal Data Controller shall generally be the most senior staff member who has decision-making authority over the personal data processing operations. When there are two or more such senior staff members, they shall be joint Personal Data Controllers.

(c) In the case of joint Personal Data Controllers, clear roles and responsibilities must be established for each Personal Data Controller with respect to the requirements and obligations set out under this Policy.

(d) The designation of a Personal Data Controller aims to enable efficient and effective compliance with UNHCR's data protection and privacy standards. Where not specified by official guidance or other instrument or practice, the designation shall consider the factual circumstances of the decision-making authority over the personal data processing, especially to avoid undue burdens in smaller country operations and entities.

68. A Personal Data Controller may designate personal data protection focal points. When the Personal Data Controller is the head of an entity for which personal data processing is a substantial or critical activity, personal data protection focal points should be designated.

(iii) Chief Data Protection and Privacy Officer (Chief DPO)

69. The Chief DPO has the authority to provide independent and impartial expert support and advice on the application of this Policy. They are accountable for global monitoring and oversight functions in order to support UNHCR's compliance with this Policy and other policies and administrative instructions relating to UNHCR's data protection and privacy framework, including through collaboration with Personal Data Controllers and with regional bureaux Directors.

70. The Chief DPO assists in the designation or determination of Personal Data Controllers and performs other roles and duties as may be assigned by the High Commissioner, which requires performance in an independent and impartial manner.

71. There will be a single Chief DPO for UNHCR who will be supported, as appropriate, by a data protection office.

(iv) Personal Data Protection Review Committee

72. The Personal Data Protection Review Committee has the authority to independently and impartially consider redress requests made by data subjects and to issue recommendations (including with respect to remedies) for final determination by the High Commissioner.

73. The Review Committee members are appointed by the High Commissioner and will include at least one member who is external to UNHCR. Members must have relevant expert capacities in the field of data protection and privacy and must exercise independent and impartial judgment. Neither the Chief DPO nor any members of the data protection office may be members of the Review Committee.

74. The High Commissioner may allocate to the Review Committee other roles and responsibilities relating to personal data protection which require performance in an independent and impartial manner.

Part 5. Entry into Effect

(i) For persons of concern

75. With respect to the personal data of persons of concern, this Policy will take effect on the date of entry into force of this Policy, subject to the following:

(a) the Policy on the Protection of Personal Data of Persons of Concern to UNHCR will be deemed an implementing instrument as contemplated by paragraph 16;

(b) the current data controllers designated under the Policy on the Protection of Personal Data of Persons of Concern to UNHCR with respect to the personal data of persons of concern will be deemed to be Personal Data Controllers for the purposes of this Policy;

(c) the current Data Protection Officer under the Policy on the Protection of Personal Data of Persons of Concern to UNHCR will act as the Chief DPO with respect to the personal data of persons of concern until the Chief DPO function is established under this Policy; and

(d) the provisions of this Policy concerning the Personal Data Protection Review Committee and the redress procedure set out in paragraphs 54 through 60 will take effect with respect to the personal data of persons of concern no later than 12 months after the date of entry into force of this Policy.

76. Annex 1 to this Policy contains transition activities to allow for coordination between UNHCR's data protection and privacy standards under this Policy and the Policy on the Protection of Personal Data of Persons of Concern to UNHCR.

(ii) For data subjects other than persons of concern

77. With respect to the personal data of data subjects other than persons of concern, this Policy will enter into effect three years after the date of entry into effect of this Policy. However, the High Commissioner may decide that this Policy come into effect prior to the end of this three-year period with respect to particular categories of data subjects.

Part 6. Final Provisions

(i) Delegation by the High Commissioner

78. The High Commission may delegate any of the responsibilities allocated to the High Commissioner under this Policy.

(ii) Public diffusion of decisions

79. Information about the decisions of the High Commissioner or the delegate of the High Commissioner in relation to the application and interpretation of the data protection and privacy standards in this Policy will be made available in a form suitable for publication.

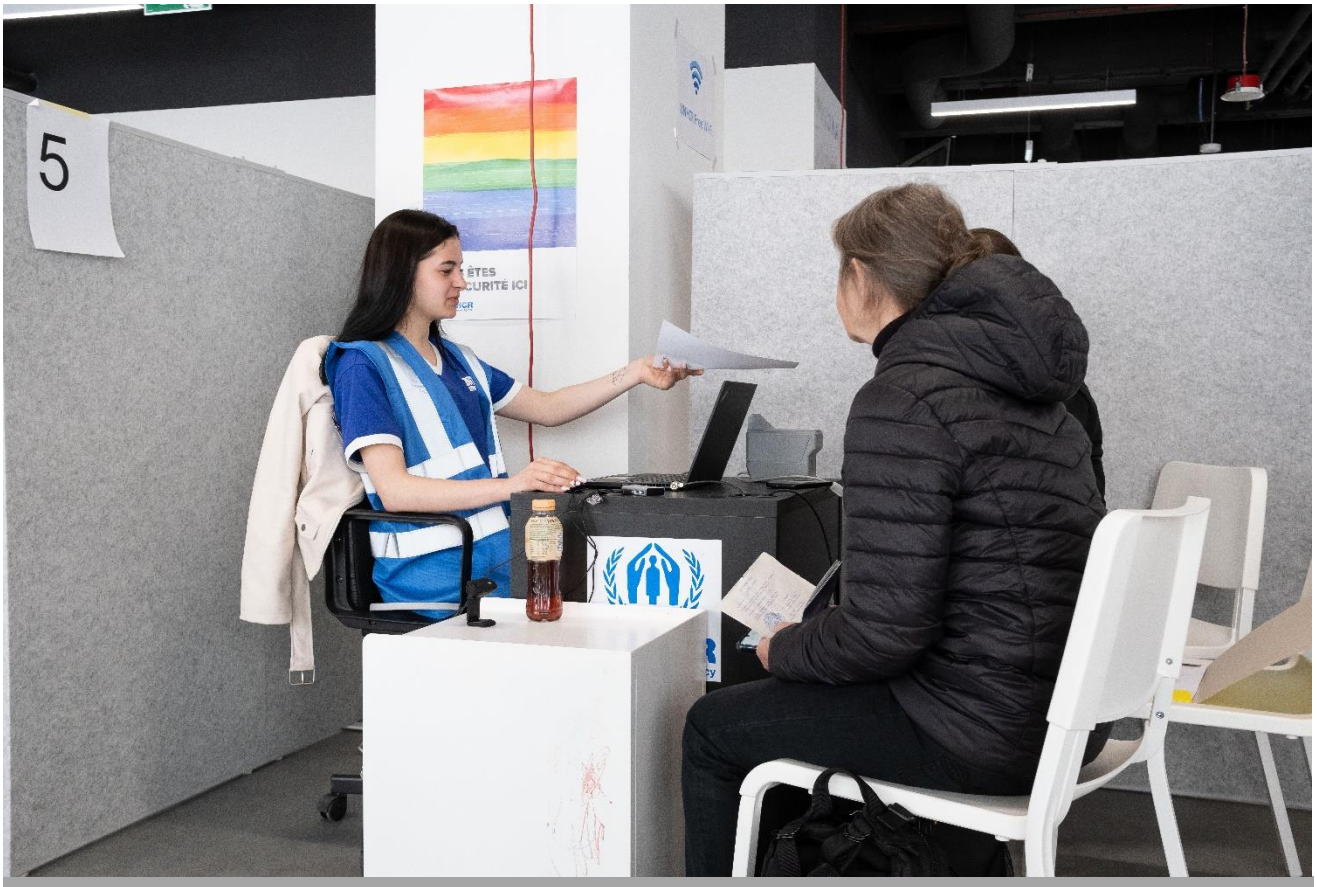
(iii) Privileges and immunities

80. This Policy is without prejudice to UNHCR's privileges and immunities under the 1946 Convention on the Privileges and Immunities of the United Nations.

(iv) Monitoring and compliance

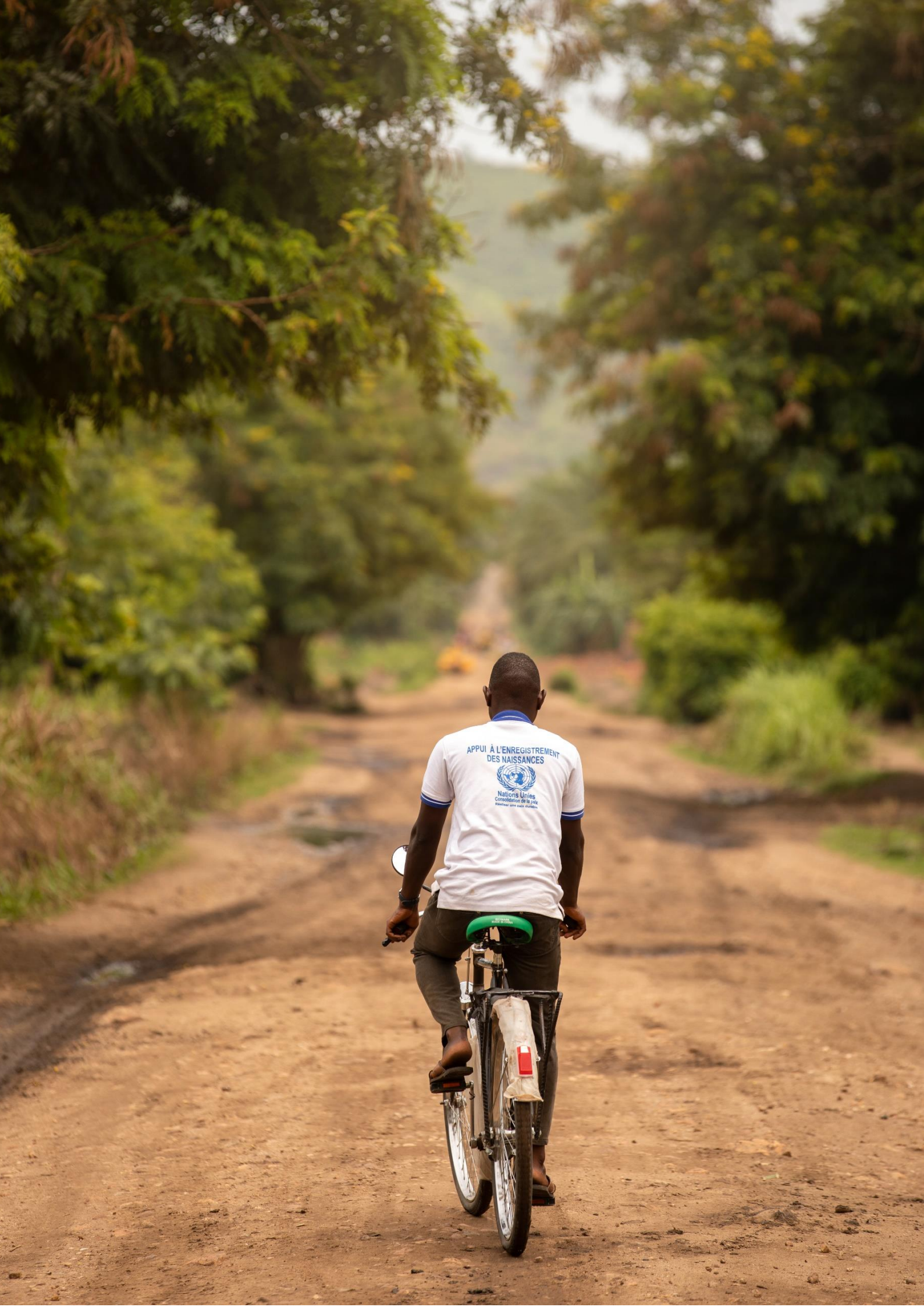
81. Compliance with this Policy will be monitored under the overall leadership and oversight of the Chief DPO, with the support of the regional bureaux in regards to their respective countries.

82. Personal Data Controllers designated at country, regional, HQ and global level will be accountable for compliance with this Policy with respect to the processing operations under their authority and will report to the Chief DPO on compliance on an annual basis. To this end, implementing instructions referred to in paragraph 16 may establish monitoring frameworks.



© UNHCR/Maciej Moskwa

(Left blank intentionally)


APPUI À L'ENREGISTREMENT
DES NAISSANCES
Nations Unies
Consolidation de la paix