POLICY

on the Protection of Personal Data of Persons of Concern to UNHCR

UNHCR
The UN Refugee Agency

DATA PROTECTION POLICY

CONTENTS

1

GENERAL PROVISIONS

1.1 PURPOSE

This Policy lays down the rules and principles relating to the processing of personal data of persons of concern to UNHCR. Its purpose is to ensure that UNHCR processes personal data in a way that is consistent with the 1990 United Nations General Assembly's *Guidelines for the Regulation of Computerized Personal Data Files*[1] and other international instruments concerning the protection of personal data and individuals' privacy. The Policy will be complemented by Operational Guidelines that will provide guidance on its implementation, supervision and accountability.

1.2 RATIONALE

1.2.1 In pursuit of its international protection and solutions mandate, and also when offering its good offices to States, UNHCR is often required to process personal data of persons of concern to the Organization. This may also include the need to share personal data with Implementing Partners and/or third parties. In processing personal data there are inherent risks such as accidental or unauthorized loss or disclosure. Given the particularly vulnerable position of persons of concern to UNHCR, the nature of their personal data is generally sensitive and, therefore, requires careful handling in line with this Policy. For UNHCR, the proper protection of the personal data of persons of concern is therefore of particular importance and the Organization

1 UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files,* as adopted by Resolution A/Res/45/95 of 14 December 1990, available at: http://www.refworld.org/docid/3ddcafaac.html.

has a responsibility to process it in a way that respects data protection principles.[2]

1.2.2 The Policy also complements the provisions of UN Staff Regulation 1.2 (i) and commitments in UNHCR's Code of Conduct, in particular, Principle 6, which calls on staff to safeguard and make responsible use of the information to which they have access.

1.3 SCOPE

1.3.1 This Policy applies to all personal data held by UNHCR in relation to persons of concern to UNHCR.[3] The processing of other data, e.g. aggregated or anonymized, does not fall within the scope of this Policy, but is covered, *inter alia*, by UNHCR's Information Classification, Handling and Disclosure Policy.

1.3.2 This Policy applies whether processing takes place within one UNHCR office, between different UNHCR offices in the same or more than one country, or whether personal data is transferred to Implementing Partners or third parties. The Policy continues to apply even after persons are no longer of concern to UNHCR.

1.3.3 Compliance with this Policy is mandatory for all UNHCR personnel.

---

2 The Executive Committee of the High Commissioner's Programme has referred to data protection principles in the following Conclusions: No. 91 (LII) – 2001 (f), available at: http://www.unhcr.org/3bd3e1d44.html; No. 93 (LIII) – 2002 (b) (viii), available at: http://www.unhcr.org/3dafdd344.html; and No. 102 (LVI) – 2005 (v), available at: http://www.unhcr.org/43575ce3e.html.

3 UNHCR, Note on the Mandate of the High Commissioner for Refugees and his Office, October 2013, available at: http://www.refworld.org/docid/5268c9474.html.

1.4 TERMS AND DEFINITIONS

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

Consent

Any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action.

Data controller

The UNHCR staff member, usually the Representative in a UNHCR country office, who has the authority to oversee the management of, and to determine the purposes for, the processing of personal data.

Data processor

Any UNHCR staff member or other natural person or organization, including an Implementing Partner or third party that carries out processing of personal data on behalf of the data controller.

Data protection focal point

In principle, the most senior UNHCR protection staff member in a UNHCR country office or operation, who assists the data controller in carrying out his or her responsibilities regarding this Policy.

Data protection impact assessment

A tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary in order to avoid or minimize such impacts.

Data Protection Officer

The UNHCR staff member in the Division of International Protection at Headquarters who supervises, monitors and reports on compliance with this Policy. Responsibilities of the Data Protection Officer are set out in Part 7.3.

Data subject

An individual whose personal data is subject to processing.

Data transfer agreement

An agreement between UNHCR and an Implementing Partner or third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

Implementing Partner

An organization established as an autonomous and independent entity from UNHCR that UNHCR engages through a project partnership agreement to undertake the implementation of programmatic activities within its mandate.

Personal data

Any data related to an individual who can be identified from that data; from that data and other information; or by means reasonably likely to be used related to that data. Personal data includes biographical data (biodata) such as name, sex, marital status, date and place of birth, country of origin, country of asylum, individual registration number, occupation, religion and ethnicity, biometric data[4] such as a photograph, fingerprint, facial or iris image, as well as any expression of opinion about the individual, such as assessments of the status and/or specific needs.

Personal data breach

A breach of data security leading to the accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transferred, stored or otherwise processed.

Person of concern

A person whose protection and assistance needs are of interest to UNHCR. This includes refugees, asylum-seekers, stateless persons, internally displaced persons and returnees.

4 Biometric data is a personal biological (anatomical or physiological) or behavioural characteristic which can be used to establish a person's identity by comparing it with stored reference data.

© UNHCR / Dalia Khamissy

Processing of personal data

Any operation, or set of operations, automated or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, transfer (whether in computerized, oral or written form), dissemination or otherwise making available, correction, or destruction.

Third party

Any natural or legal person other than the data subject, UNHCR or an Implementing Partner. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

2

BASIC PRINCIPLES

2.1 BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

UNHCR personnel need to respect and apply the following basic principles when processing personal data:

(i) Legitimate and fair processing

(ii) Purpose specification

(iii) Necessity and proportionality

(iv) Accuracy

(v) Respect for the rights of the data subject

(vi) Confidentiality

(vii) Security

(viii) Accountability and supervision

2.2 LEGITIMATE AND FAIR PROCESSING

Processing of personal data may only be carried out on a legitimate basis and in a fair and transparent manner. UNHCR may only process personal data based on one or more of the following legitimate bases:

(i) With the consent of the data subject

(ii) In the vital or best interests of the data subject

(iii) To enable UNHCR to carry out its mandate

(iv) Beyond UNHCR's mandate, to ensure the safety and security of persons of concern or other individuals

2.3 PURPOSE SPECIFICATION

Personal data needs to be collected for one or more specific and legitimate purpose(s) and should not be processed in a way incompatible with this/those purpose(s).

2.4 NECESSITY AND PROPORTIONALITY

The processing of personal data should be necessary and proportionate to the purpose(s) for which it is being processed. Therefore, data that is processed should be adequate and relevant to the identified purpose, and not exceed that purpose.

2.5 ACCURACY

Personal data should be recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.

2.6 RESPECT FOR THE DATA SUBJECT'S RIGHTS

The data subject's rights to information, access, correction, deletion and objection, are dealt with under Part 3 of this Policy.

2.7 CONFIDENTIALITY

UNHCR personnel need to maintain the confidentiality of the personal data of persons of concern at all times, even after a data subject is no longer of concern to UNHCR.

2.8 SECURITY

In order to ensure the confidentiality and integrity of personal data, appropriate technical and organizational data security measures need to be put in place. Data security and other related issues are dealt with in Part 4. Transfer of personal data to third parties is limited to the conditions set out in Part 6.

2.9 ACCOUNTABILITY AND SUPERVISION

In order to ensure accountability for the processing of personal data in line with this Policy, UNHCR will set up an accountability and supervision structure as set out in Part 7.

3

RIGHTS OF THE DATA SUBJECT

3.1 INFORMATION

When collecting personal data from a data subject, UNHCR should inform the data subject of the following, in writing or orally, and in a manner and language that is understandable to the data subject:

(i) The specific purpose(s) for which the personal data or categories of personal data will be processed;

(ii) Whether such data will be transferred to Implementing Partner(s) or third parties or, where the data is being collected by an Implementing Partner on behalf of UNHCR, that the data subject is informed of this fact;

(iii) The importance of the data subject providing accurate and complete information;

(iv) The data subject's duty to keep UNHCR, and/or, as appropriate, Implementing Partners, informed of changes to their personal situation;[5]

(v) Any consequences for refusing or failing to provide the requested personal data;

(vi) The data subject's right to request access to their personal data, or correction or deletion of it;

(vii) The data subject's right to object to the collection of personal data;

(viii) How to lodge a complaint with the data controller and with the Inspector General's Office.

5 In particular, changes in civil status, e.g. births, deaths and marriages.

3.2 ACCESS

Upon request the data subject may receive from UNHCR:

(i) Confirmation as to whether or not data related to him or her has been, is being or will be processed; and

(ii) Information on the personal data being processed, the purpose(s) for processing such data and the Implementing Partner(s) and/or third parties to whom such data has been, is being or will be transferred.

3.3 CORRECTION AND DELETION

3.3.1 The data subject may request the correction or deletion of personal data that is inaccurate, incomplete, unnecessary or excessive.

3.3.2 Where a data subject requests the correction or deletion of his or her personal data, UNHCR is to request proof relating to the inaccuracy or incompleteness.

3.4 OBJECTION

Subject to Part 3.7 below, a data subject may object to the processing of his or her personal data where there are legitimate grounds related to his or her specific personal situation. If the objection is justified, UNHCR should no longer process the personal data concerned.

3.5 MODALITIES OF REQUESTS

3.5.1 Requests for information about access to, correction or deletion of personal data or an objection, may be made by the data subject or his or her authorized legal representative, or, in the case of a child, a parent or legal guardian. Requests are to be submitted orally or in writing to the UNHCR office in the country where the data is being processed.

3.5.2 Before complying with any request or objection, UNHCR should satisfy itself of the identity of the person making the request or objection. The individual is required to identify him or herself in an appropriate manner. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and objections from parents or guardians for children should be evaluated against the best interests of the child.

3.6 RECORDING AND RESPONSE BY UNHCR

3.6.1 UNHCR is to record the fact of having provided the data subject with the information pursuant to Part 3.1 as well as to record requests received for access, correction, deletion or objection and the response provided in relation to such requests pursuant to Parts 3.2, 3.3 and 3.4.

3.6.2 UNHCR is to respond to a request or objection under Part 3 within a reasonable time, in writing or orally, and in a manner and language that is understandable to the data subject and/or his or her legal representative or legal guardian, as applicable.

© UNHCR / M. Abu Asaker

3.7 RESTRICTIONS

Based on consultations with the Data Protection Officer, and other relevant counterparts at Headquarters, UNHCR may refuse to provide a response or limit or restrict its response to a request or objection under Part 3 where:

(i) It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following:

(a) The safety and security of UNHCR, its personnel or the personnel of Implementing Partners; or

(b) The overriding operational needs and priorities of UNHCR in pursuing its mandate.

(ii) There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

4

DATA PROCESSING BY UNHCR

4.1 CONFIDENTIALITY OF PERSONAL DATA

4.1.1 Personal data is by definition classified as confidential. The confidentiality of personal data must be respected by UNHCR when processing personal data at all times.

4.1.2 In order to ensure and respect confidentiality, personal data must be filed and stored in a way that it is accessible only to authorized personnel and transferred only through the use of protected means of communication.

4.2 SECURITY OF PERSONAL DATA

4.2.1 UNHCR needs to ensure and implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data, the availability and quality of the necessary equipment, the cost and the operational feasibility.

4.2.2 UNHCR's data security measures are to protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

4.2.3 Having regard to the available technology and the cost of implementation, UNHCR needs to implement appropriate organizational and technical measures to ensure that the processing meets the requirements of this Policy. This includes the implementation of data protection enhancing technologies and tools to enable data processors to better protect personal data ("privacy by design and by default").

4.2.4 Organizational measures include:

(i) Setting up Standard Operating Procedures;

(ii) Organizing staff training in data protection and security; and

(iii) Conducting data protection impact assessments (Part 4.5).

4.2.5 Technical measures include:

(i) Maintaining physical security of premises, portable equipment, individual case files and records;

(ii) Maintaining computer and information technology (IT) security, for example, access control (e.g. passwords, tiered access), user control, storage control, input control, communication and transport control (e.g., encryption).

4.2.6 In deteriorating security situations that pose a serious risk of personal data breaches, UNHCR should take all necessary and possible steps to avoid such personal data breaches, by relocating, or, as a matter of last resort, destroying individual case files, whether in paper or computerized form, that contain personal data, in order to prevent harm to data subjects.

4.3 ENSURING ACCURACY OF PERSONAL DATA

4.3.1 UNHCR may correct or delete personal data held on its systems that is inaccurate, incomplete, unnecessary or excessive.

4.3.2 UNHCR should update personal data records when necessary and periodically verify them.

4.3.3 When personal data is corrected or deleted in UNHCR's systems, UNHCR should notify, as soon as reasonably practicable, all Implementing Partners and/or third parties to whom the relevant personal data was transferred.

4.4 NOTIFICATION OF A PERSONAL DATA BREACH

4.4.1 UNHCR personnel are required to notify the data controller as soon as possible upon becoming aware of a personal data breach and to properly record the breach.

4.4.2 If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller should use his or her best efforts to communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay. In such cases, the data controller should also notify the Data Protection Officer of the personal data breach.

4.4.3 The notification should describe:

(i) The nature of the personal data breach, including the categories and number of data subjects and data records concerned;

(ii) The known and foreseeable adverse consequences of the personal data breach; and

(iii) The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

4.5 DATA PROTECTION IMPACT ASSESSMENTS

4.5.1 When elaborating new systems, projects or policies or before entering into data transfer arrangements with Implementing Partners or third parties which may negatively impact on the protection of personal data of persons of concern, UNHCR needs to carry out a Data Protection Impact Assessment (DPIA). A DPIA is required where the collection and processing or transfer of personal data is likely to be large, repeated or structural (i.e. where data is shared with an Implementing Partner or third party over a certain period of time).

4.5.2 A DPIA would contain a general description of the envisaged system, project, policy or data sharing arrangement involving processing of personal data, an analysis of the risks to the rights of data subjects by virtue of the circumstances and the nature of the personal data processed, the safeguards, security and other measures in place or proposed to ensure the compliance with this Policy.

4.5.3 Data controllers are responsible for organising and carrying out DPIAs, when required. DPIAs are normally carried out at the country level unless it is decided that a DPIA is to be carried out at global or regional level due to the scope of system or arrangement.

4.5.4 Data controllers are to keep the Data Protection Officer fully informed of any DPIA carried out under their responsibility and to share a copy of the DPIA.

4.6 RETENTION

4.6.1 Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purpose(s) for which it was collected.

4.6.2 All individual case files, whether open or closed, are considered permanent records, and must therefore be permanently retained in line with the Access Policy of UNHCR Archives.[6]

6 UNHCR's Access Policy, available at: http://www.unhcr.org/3b03896a4.html.

5

DATA PROCESSING BY IMPLEMENTING PARTNERS

5.1 GENERAL CONDITION

Where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed on behalf of UNHCR. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection as contained in this Policy (in particular Parts 2, 3 and 4). This applies whether UNHCR intends to transfer personal data to Implementing Partners or Implementing Partners collect personal data in order to carry out agreed activities.

5.2 VERIFICATION

Irrespective of a partnership agreement, UNHCR needs to verify, prior to transferring personal data to an Implementing Partner or to engaging an Implementing Partner in the collection and processing of personal data, that the processing of personal data by the Implementing Partner satisfies the standards and basic principles of this Policy. Such verification may form part of a Data Protection Impact Assessment.

© UNHCR / Frederic Noy

5.3 PARTNERSHIP AGREEMENTS

UNHCR is to require Implementing Partners to comply with this Policy through an undertaking as part of the signing of partnership agreements. Such agreements also need to specify the specific purpose(s) for the processing of personal data and the legitimate basis for processing.

5.4 CAPACITY OF THE PARTNER

UNHCR may need to assist Implementing Partners in building or enhancing their capacity in order to comply with the data protection standards and principles contained in this Policy. Such assistance may relate to the establishment or adjustment of policies, the delivery of training or putting in place technical and organizational measures.

5.5 PARTNERSHIP TERMINATION

After termination of a partnership, all personal data collected in the performance of the partnership would be returned to UNHCR. Partnership agreements may provide for exceptions, in particular where there are legitimate reasons to do so, namely consent of the data subjects.

6

TRANSFER OF PERSONAL DATA TO THIRD PARTIES

6.1 GENERAL CONDITIONS

6.1.1 UNHCR may transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy.

6.1.2 Given the potential data protection risks involved in transfers to third parties, UNHCR needs to pay particular attention to the following basic principles of this Policy:

(i) Transfer is based on one or more legitimate bases;

(ii) Transfer is for one or more specific and legitimate purpose(s);

(iii) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;

(iv) The data subject has been informed, either at the time of collection in accordance with Part 3.1, or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions in Part 3.7 apply;

(v) The third party respects the confidentiality of personal data transferred to them by UNHCR. Whether or not a data transfer agreement has been signed between UNHCR and the third party, UNHCR must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication;

(vi) The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it.

6.1.3 In addition, UNHCR needs to ensure that transferring personal data does not negatively impact:

(i) the safety and security of UNHCR personnel and/or personnel of Implementing Partners; and/or

(ii) the effective functioning of an UNHCR operation or compromise UNHCR's mandate, for example due to the loss of the climate of trust and confidence between UNHCR and persons of concern or the loss of the perception of UNHCR as an independent, humanitarian and non-political Organization.

6.1.4 Before agreeing to transfer personal data to a third party, UNHCR needs to assess the level of data protection afforded by the third party. As part of this assessment, the data controller should assess, *inter alia,* the applicable laws and regulations, internal statutes and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as the technical and organizational means of data security put in place. Pursuant to Part 4.5, the data controller may need to carry out a DPIA.

6.2 DATA TRANSFER AGREEMENTS

6.2.1 Unless there are satisfactory reasons not to do so, prior to transferring personal data to a third party, the data controller should seek to sign a data transfer agreement, or, as appropriate, incorporate data protection clauses within broader agreements, particularly where transfers of personal data are likely to be large, repeated, or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time.

6.2.2 Data transfer agreements should, *inter alia:*

(i) address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;

(ii) require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and

(iii) stipulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

6.2.3 The Data Protection Officer and the Legal Affairs Service (LAS) are to review and clear all data transfer agreements. Copies of final agreements are to be lodged with the Data Protection Officer.

6.3 TRANSFER TO NATIONAL LAW ENFORCEMENT AGENCIES AND COURTS

6.3.1 In appropriate circumstances, UNHCR may transfer personal data to a national law enforcement agency or a national court. Such transfers may be upon request by the law enforcement agency or court, or on UNHCR's own initiative. Transfers may concern persons subject to an investigation for an allegedly committed crime, or in relation to the victim(s) of or witness(es) to a crime.

6.3.2 In addition to the general conditions for transferring personal data to third parties (Part 6.1, with the exception of 6.1.2 (iv)), UNHCR may only cooperate with such a request and transfer personal data to a national law enforcement agency or national court if the following conditions are met:

(i) Transfer is necessary for the purposes of the detection, prevention, investigation, or prosecution of a serious criminal offence, in particular in order to avoid an immediate and substantial risk to the safety and security of an individual or the public;

(ii) the requesting law enforcement agency or court is competent in relation to the detection, prevention, investigation or prosecution of the offence in question;

(iii) The transfer will substantially assist the law enforcement agency or court in the pursuit of these purposes and that the personal data cannot otherwise be obtained from other sources;

(iv) Transfer does not disproportionately interfere with a data subject's or another person of concern's right to privacy or other human rights; and

(v) In the case of data in relation to victims and witnesses, their consent to the transfer has been obtained.

6.3.3 Prior to the transfer of personal data to a national law enforcement agency or a national court, advice from the Data Protection Officer, in consultation with the Protection and National Security Unit within the Division of International Protection, LAS and the concerned Bureau(s), needs to be sought.

6.4 INTERNATIONAL LAW ENFORCEMENT AGENCY, INTERNATIONAL COURT, TRIBUNAL OR OTHER INTERNATIONAL BODY

Requests for transfers of personal data by the International Criminal Court, *ad hoc* international criminal tribunals, UN-mandated commissions of inquiry and similar international bodies are to be referred to the Division of International Protection (Data Protection Officer, Protection and National Security Unit and Human Rights Liaison Unit as appropriate) and LAS.

6.5 PRIVILEGES AND IMMUNITIES

The transfer of personal data is without prejudice to the UNHCR's privileges and immunities under the 1946 *Convention on the Privileges and Immunities of the United Nations* and should not be construed as doing so. Privileges and immunities of UNHCR and its staff members exist regardless of any cooperation agreement with the Government of a country. Any queries on privileges and immunities are to be addressed to UNHCR's LAS.

7

ACCOUNTABILITY AND SUPERVISION

7.1 ACCOUNTABILIY AND SUPERVISION STRUCTURE

UNHCR's accountability and supervision structure referred to in Part 2.9 will consist of the following key actors:

(i) A Data Protection Officer within the Division of International Protection at UNHCR Headquarters,

(ii) Data controllers in each country office/operation, and

(iii) Data protection focal points in country offices/ operations.

7.2 DATA CONTROLLER AND DATA PROTECTION FOCAL POINT

7.2.1 The data controller is responsible for establishing and overseeing the processing of personal data under his or her area of responsibility. He or she therefore also bears the main responsibility for compliance with the Policy. To that end, the data controller should designate a data protection focal point. The data protection focal point should in principle be the most senior UNHCR protection staff member in a country office/operation.

7.2.2 The data controller, assisted by the data protection focal point, is to implement this Policy by, *inter alia:*

(i) Determining the applicable legitimate basis for and the specific and legitimate purposes of data processing;

(ii) Ensuring the implementation of organizational and security measures as well as assessing data security of third parties;

(iii) Establishing internal procedures, for example in the form of Data Protection Standard Operating Procedures, covering all relevant aspects of this Policy, in particular regarding the respect for the rights of the data subject and measures aimed at ensuring data confidentiality and security;

(iv) Ensuring that data protection and data security aspects are adequately included in Implementing Partner agreements;

(v) Negotiating and concluding data transfer agreements with third parties as required or appropriate.

7.2.3 As necessary, the data controller and/or data protection focal point should seek the advice of the Data Protection Officer concerning queries with regard to the application and interpretation of this Policy.

7.3 DATA PROTECTION OFFICER

7.3.1 UNHCR will appoint a Data Protection Officer based in the Division of International Protection at UNHCR Headquarters, whose tasks will include:

(i) Providing advice, support and training on data protection and this Policy;

(ii) Maintaining inventories of information provided by data controllers and data protection focal points, including data transfer agreements, specific instances of data sharing by UNHCR with third parties, data protection impact assessments, data breach notifications and complaints by data subjects;

(iii) Actively encouraging data controllers and other relevant actors to undertake measures aimed at compliance with this Policy;

(iv) Monitoring and reporting on compliance with this Policy;

(v) Liaising with LAS as necessary under this Policy.

7.3.2 The Data Protection Officer will submit an annual data protection report, through the Director of the Division of International Protection, to the Assistant High Commissioner for Protection.

7.4 INSPECTOR GENERAL'S OFFICE

This Policy does not affect the mandated function of the Inspector General's Office (IGO), notably to receive complaints of alleged misconduct, e.g. for breach of confidentiality or fraud, and to undertake investigations into such misconduct.[7] In doing so, the IGO complements the monitoring and compliance structure established by this Policy.

7.5 ETHICS OFFICE

In support of this Policy, the Ethics Office will provide guidance on ethical practices and standards and assist in mitigating the risks relating to the processing of personal data through enforcement of UNHCR's Code of Conduct, and UNHCR's Policy on Protection of Individuals Against Retaliation ('Whistle-blower policy').

7 Information on the function of the IGO and how to make a complaint is available at: http://www.unhcr.org/pages/52e11b746.html.

© UNHCR / Jared Kohler