DATA MANAGEMENT AND PROTECTION

IMPROVING CASH-BASED INTERVENTIONS
MULTIPURPOSE CASH GRANTS AND PROTECTION
Enhanced Response Capacity Project 2014–2015

Privacy Impact Assessment of UNHCR Cash Based Interventions

UNHCR
The UN Refugee Agency

Trilateral Research & Consulting

Privacy Impact Assessment of UNHCR Cash Based Interventions

December 2015

This document was written for the Office of the United Nations High Commissioner for Refugees by TriLateral Research and Consulting.

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.

Contents

CONTENTS

Acronyms

ATM	Automated Teller Machine
CBIs	Cash Based Interventions
DPA	Data Protection Authority
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technologies
INGO	International Non-Governmental Organisation
IGO	Inter-Governmental Organisation
ISO	International Organization for Standardization
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
PoC	Persons of Concern
PIA	Privacy Impact Assessment
PII	Personally identifiable information
SOPs	Standard Operating Procedures
UNHCR	Office of the United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
WASH	Water, Sanitation and Hygiene
WFP	World Food Programme

1 Introduction

Information about refugees, asylum seekers, internally displaced persons and other persons of concern (PoCs) is open to misuse or abuse if not properly protected. The use of cash-based interventions (CBIs) emphasise existing data protection challenges for United Nations agencies, and other agencies providing cash assistance because personal information must be augmented and shared with third parties. These challenges must be addressed if data controllers[1] are to meet their data protection obligations and minimise the risk to their beneficiaries' fundamental right to privacy.

In 2014, the Office of the United Nations High Commissioner for Refugees (UNHCR) commissioned Trilateral Research & Consulting to conduct privacy impact assessments (PIAs) of two of its CBIs in middle-income countries. The purpose of the PIAs was to help UNHCR assess the specific data protection and privacy risks arising from the collection, processing, storage and sharing of personally identifiable information (PII)[2] relating to refugees and other PoCs by country operations and its transfer to partners involved in the implementation of CBIs. The complexity of large-scale CBIs has brought data protection and privacy issues to the forefront of UNHCR operations. These PIAs are among various initiatives by UNHCR to enhance beneficiary privacy, including the recent adoption of a global data protection policy.[3] This report presents the findings of the PIAs of CBIs in the two UNHCR country operations. The report also highlights key issues related to data protection that go beyond CBIs and are equally relevant to in-kind assistance, and need to be addressed globally. Since cash assistance involves multiple actors and stakeholders, many of the report's recommendations will be relevant to other humanitarian actors with CBIs or similar assistance programmes. However, it should be noted that country-level findings may not be applicable to CBIs in other UNHCR operations.

The following section of the report (Section 2) examines the key features and challenges of CBIs and introduces the privacy and data protection challenges they pose. Section 3 explains the PIA process and the benchmarks that data controllers should strive to meet. Section 4 maps the information flows in the two CBIs assessed by Trilateral. Section 5 sets out the privacy risks associated with the information flows, identifies key threats and vulnerabilities, and sketches the key findings of the PIAs. Section 6 contains the principal recommendations stemming from the PIAs. Because the information flows examined in the PIA process necessarily went beyond the CBIs to the datasets that underpin them (e.g., registration data), the recommendations address organisation-wide data protection and beneficiary privacy matters as well as specific issues related to CBIs. Since work began on this report, UNHCR has implemented most of the recommendations.

[1] A data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which personal data is processed by or on behalf of their organisation.

[2] Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

[3] UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR, May 2015. www.refworld.org/docid/55643c1d4.html

2 Key features of cash-based interventions

Cash and voucher transfers are increasingly used by humanitarian organisations in response to emergencies because they are often quick to deliver, cost-effective and provide people in need of support with greater choice.

UNHCR has long used cash grants and vouchers and is today pioneering new CBIs for refugees. In the 1980s and 1990s, UNHCR typically used cash interventions to assist refugees returning to their country of origin. More recently, a focus on alternatives to refugee camps and the increasing number of humanitarian crises and displaced persons has necessitated new ways of reaching out to those in need of protection and assistance in an efficient and effective manner.

Today, CBIs are "an important tool in such settings, going hand in hand with harnessing new technologies, fostering partnerships within and beyond the humanitarian community, and tapping into existing systems to deliver assistance and protection, including public-private partnerships and national social protection schemes". [4]

This combination of new assistance modalities, new technologies and multiple partnerships has produced novel challenges for UNHCR in the collection, storage, processing and transfer of refugee data. In the wrong hands, such data can impact a refugee's safety as much as any other economic, social or political risk.

CBIs can be sector-specific or multi-purpose intended to meet multiple needs. UNHCR's unconditional cash assistance in the two operations studied targets the most economically vulnerable refugees and provides them with money to help meet their basic needs. The aim is to close the gap between refugees' incomes and the recognised poverty line or estimated local "minimum expenditure basket".

Evaluations of CBIs have been largely positive, with benefits seen to include greater dignity (through choice) for recipients and a multiplier effect in local economies. In 2011, just over a third of UNHCR country operations operated cash assistance programmes; in 2012, UNHCR encouraged all operations to consider such interventions in their yearly programming cycle.[5] Although UN agencies have implemented cash assistance in larger emergency responses since 2010, the majority of CBIs are relatively small scale.

UNHCR supports the targeting and delivery of cash and in-kind interventions by partner agencies including the World Food Programme (WFP), the UN Children's Fund (UNICEF) and other active international humanitarian non-governmental organisations (NGOs) and international NGOs (INGOs) by providing them with PoCs' personal data.[6] The involvement of multiple partners and datasets in cash assistance programming amplifies the privacy and data protection risks faced by UNHCR and the people it supports.

In order to determine eligibility for cash assistance, UNHCR and its partners are using new data aggregation, profiling and social sorting techniques,[7] which may increase these concerns.

4 UNHCR, An Introduction to Cash-Based Interventions in UNHCR Operations, March 2012. www.unhcr.org/515a959e9.pdf

5 Ibid.

6 Data that may be shared varies depending on the mandate of the co-operating organisation but should be limited to basic contact, biographical and needs assessment information.

7 In data protection, 'profiling' means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements. See further Article 29 Data Protection Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation. May 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf. Social sorting is a phenomenon of surveillance systems that obtain personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access and so on. See Lyon, David, "Surveillance as social sorting", in David Lyon (ed.), Surveillance as social sorting, Routledge, London, 2003, p. 20.

Cash distribution modalities have important implications for how personal data is collected, shared and stored. Where it is safe and practical to do so, beneficiaries should be able to access cash directly from bank ATMs (automated teller machines) and spend it as they choose. Alternative distribution options include pre-loaded debit cards, e-vouchers, partnerships with supermarkets and direct cash transfers. The World Bank and major European donors support cash assistance programmes in the context of a broader trend toward the "monetisation of aid".[8]

However, despite their use in many countries, "the use of cash and vouchers in humanitarian response is still not institutionalised nor the important step of modality selection systematically considered".[9] The climate in which UNHCR's CBIs are being developed and implemented remains challenging and new targeting methodologies are still being devised both by country operations and globally.

In more protracted and larger-scale situations, humanitarian assistance programing accrues many of the characteristics of traditional social security and welfare programmes. This brings with it corresponding challenges in terms of eligibility and entitlement, fraud and abuse, and data protection.

UNHCR and its partners are also under pressure to make cash assistance more efficient by improving co-operation and harmonising operational modalities with partners in the humanitarian community. The processes of determining eligibility and disbursing funds can involve multiple assessments of household welfare, the creation of vulnerability profiles and the use of diverse financial partners. The use of econometric modelling, 'big data' analytics[10] and biometric technologies, which are used to verify the identity of beneficiaries, also pose challenges in terms of ensuring data privacy and compliance with UNHCR's data protection policy.

3 The PIA process

A PIA is a process for assessing the impacts on privacy of a project, policy, programme, product or service and, in consultation with stakeholders, for taking remedial actions as necessary in order to correct, avoid or minimise the negative impacts on data subjects.[11] One size does not fit all; PIAs provide a model for assessment that can be adapted to suit the specific needs and requirements of the organisation or project. The PIA should not simply stop once an organisation has "ticked the boxes". Assessment and review should be cyclical rather than linear, and include accountability towards those who will be using and/or are subject to the system or technology.

3.1 Methodology

Conducting a PIA of large-scale UNHCR CBIs was a substantial undertaking because of the numerous data flows, partners and processes involved. These include the registration of refugees, the identification of beneficiaries, the assessment of eligibility, the disbursement of funds, the monitoring of impact, and the auditing of programme implementation. Moreover, a PIA is often carried out during the development stage of a project or programme. Carrying out a PIA when programmes are already operational inevitably means that the PIA process is more complicated. Nevertheless, a PIA still performs a critical function in already established systems by identifying problems and solutions.

[8] See, for example, European Commission Directorate General ECHO, "The Use of Cash and Vouchers in Humanitarian Crises", Funding Guidelines 2014. http://ec.europa.eu/echo/files/policies/sectoral/ECHO_Cash_Vouchers_Guidelines.pdf

[9] DG ECHO funding guidelines, March 2013.

[10] 'Big data' analytics refers to the process of examining large data sets containing a variety of data types to uncover patterns, correlations, trends, preferences and other potentially useful information.

[11] Wright, David, "The state of the art in privacy impact assessment", Computer Law & Security Review, Vol. 28, No. 1, Feb. 2012, pp. 54-61 [p. 55]. The International Organization for Standardization (ISO) has adopted the definition in its current draft standard on privacy impact assessment (WD29134).

Trilateral has developed best practices for conducting PIAs.[12] Its methodology ensures that privacy issues and risks are analysed and addressed, but is flexible enough to respond to particular organisational and programmatic challenges. The PIAs conducted for two of UNHCR's CBIs consisted of three main stages. The first stage consisted of a brief, high-level analysis based on the programme objectives, standard operating procedures and other policy documents, together with a basic stakeholder analysis. This provided a framework to further analyse policy and practice, to identify privacy and security risks, to raise awareness of data protection and privacy issues, and to reduce both the occurrence and consequence of information security breaches.

The second stage of the PIAs consisted of field missions to the two country operations identified for the assessment in order to interview internal and external stakeholders, to observe the information flows, to assess policy and practice, and to gather the supplementary information required to evaluate the CBIs. Trilateral used a flexible, semi-structured format for interviews and guaranteed anonymity to respondents in order to solicit free and unconstrained responses.

Trilateral used the empirical data collection in the third phase of the PIA to map the information flows, to analyse the data collected from the interviews and supplementary documentation, to identify practical problems and conduct a fuller risk assessment. This final stage of the PIA was designed to help UNHCR minimise privacy risks and develop solutions in areas of concern.

3.2 Benchmarks for privacy and data protection

All humanitarian organisations processing sensitive personally identifiable data about refugees and other persons of concern should strive to meet the highest data protection standards. PIAs use benchmarks derived from international law, standardisation bodies and best practice to assess the performance of organisations and their data processing operations. Privacy is a fundamental human right and data controllers are obliged to protect datasets containing personal information. The protection of a refugee's personal information is particularly important due to the sensitive nature of the data and the potential for serious misuse of that information. At the time Trilateral conducted the PIAs, the UNHCR had not yet finalised its data protection policy, which was adopted in the spring of 2015.[13] Nevertheless, key data protection principles as described in section 3.2.2. (below) had been incorporated into some UNHCR standard operating procedures (SOPs), for example, the SOPs governing the registration process. However, in the absence of an organisation-wide data protection policy at the time, the following benchmarks were used in the PIAs as a baseline against which to assess the data processing operations underpinning UNHCR's CBIs.

3.2.1 The right to privacy

The right to privacy is enshrined in various international accords including the Universal Declaration on Human Rights 1948; the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980; the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1980; the European Data Protection Directive 95/46/EC; and the APEC Privacy Framework 2004. Article 12 of the United Nations Universal Declaration on Human Rights 1948 stipulates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". The UN also recognised the right to privacy under Article 17 of the

[12] Ibid. See also Kroener, Inga, and David Wright, "A strategy for operationalising privacy by design", The Information Society, Vol. 30, No. 5, 2014, pp. 355–365.

[13] UN High Commissioner for Refugees (UNHCR), Policy on the Protection of Personal Data of Persons of Concern to UNHCR, Geneva, May 2015. www.refworld.org/docid/55643c1d4.html

International Covenant on Social and Political Rights and Article 16 of the Convention on the Rights of the Child, which states: "(1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation; (2) The child has the right to the protection of the law against such interference or attacks".

3.2.2 The right to data protection

A growing number of countries also recognise individuals' right to data protection, most notably those in the European Union (EU), which continues to legislate in this area. In addition to the right to privacy as set out in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (to which all EU Member States are bound), Article 8 of the EU Charter of Fundamental Rights states: "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

National data protection law is based on eight core principles set out in the Directive 95/46/EC on the collection and processing of personal data in the EU, under which data must be (i) fairly and lawfully processed; (ii) processed for limited purposes; (iii) adequate, relevant and not excessive; (iv) accurate; (v) not kept for longer than necessary, (vi) processed in accordance with the individual's rights; (vii) secure; and (viii) not transferred to countries without protection. Since 2012, the EU has been negotiating a replacement data protection law that aims to raise and supplement these standards. In particular, the draft General Data Protection Regulation (GDPR) will extend data protection to include a "right to be forgotten", will give individuals the right to decide when they no longer want their data to be processed (and enforce deletion), and set expiry dates with regard to the deletion of data. It also provides for consent to be given explicitly rather than be assumed, and gives individuals the right to refer complaints to their national data protection authority (DPA), even when their personal data is processed outside their home country. Companies and organisations will have to notify customers and DPAs of serious data breaches without undue delay, and data controllers will have to ensure that privacy protections are applied throughout the entire life cycle of a product or information service. The draft GDPR also provides for mandatory data protection impact assessment (DPIA) where data processing presents serious risks to data subjects.

Guidance from the EU's Working Party on Data Protection relating to the processing of biometric information (such as fingerprints and iris scans) was also taken into account in the PIAs.[14]

3.2.3 International standards

Standards developed by the International Organization for Standardization (ISO) also provide benchmarks for PIAs. In particular, ISO/IEC 27001:2013 is an information security management standard designed to help organisations examine security risks and vulnerabilities, and to aid in the design and implementation of corresponding security controls. ISO/IEC 27005 provides further guidance on risk assessment, monitoring and review of information security management systems, while ISO 29100 sets out a list of privacy principles.

[14] "The collection, processing and storage of physiological characteristics require extra attention in any data protection policy, due to the potential impact on bodily and informational privacy." Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, Brussels, 20 June 2007. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

3.2.4 Cash Learning Partnership best practice

The Cash Learning Partnership (CaLP) has developed a growing body of expertise and guidance tailored to CBIs. This includes guidance on privacy issues, including a model PIA, and eight principles and operational standards for the secure use of personal data in cash and e-transfer programmes, which embody the core best practices discussed above. Issued in November 2013,[15] these are:

1 Organisations should respect the privacy of beneficiaries and recognise that obtaining and processing their personal data represents a potential threat to that privacy.

2 Organisations should "protect by design" the personal data they obtain from beneficiaries either for their own use or for use by third parties for each cash or e-transfer programme they initiate or implement.

3 Organisations should analyse, document and understand the flow of beneficiary data for each cash or e-transfer programme they initiate or implement within their own organisation and between their organisation and others and develop risk mitigation strategies.

4 Organisations should ensure the accuracy of the personal data they collect, store and use, including by keeping information up to date, relevant and not excessive in relation to the purpose for which it is processed, and by not keeping data for longer than is necessary.

5 At the point of data capture, beneficiaries should be informed as to the nature of the data being collected, with whom it will be shared, who is responsible for the secure use of their data and be provided with the opportunity to question the use made of the data and withdraw from the programme should they not wish their personal data to be used for the purposes described.

6 Organisations should implement appropriate technical and operational security standards for each stage of the collection, use and transfer of beneficiary data to prevent unauthorised access, disclosure or loss.

7 Organisations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so, otherwise data held by the organisation and any relevant third parties should be destroyed.

8 Organisations should establish a mechanism whereby a beneficiary can request information about what personal data an organisation holds about them, and mechanisms to receive and respond to any complaints or concerns beneficiaries may have about the use of their personal data.

3.3 Stakeholder analysis

Identifying stakeholders is a vital part of conducting a privacy impact assessment. The earlier a consultation process begins, the more benefits an organisation can expect to draw from it. Involving as wide a range of stakeholders as possible provides the opportunity to collect information on potential privacy risks and means to mitigate them; analyse information security protocols; avoid or reduce the occurrence and consequence of potential data breaches, raise awareness of data protection and privacy issues.

In the PIAs conducted by Trilateral, the following stakeholders were identified and interviewed where possible: protection, programme, data management and IT staff; their implementing, operational and financial partners (those with whom data is shared); the beneficiaries of CBIs; information and communication technology (ICT) suppliers; donors; auditors; NGOs concerned with refugee welfare.

[15] CaLP, Protecting beneficiary privacy: Principles and operational standards for the secure use of personal data in cash and e-transfer programmes, November 2013. www.cashlearning.org/resources/library/389-protecting-beneficiary-privacy-principles-and-operational-standards-for-the-secure-use-of-personal-data-in-cash-and-e-transfer-programmes

4 Information flows and data transfers

This section describes the information flows and data processing arrangements that underpin the two UNHCR CBIs subject to the PIAs.[16] Trilateral distinguished four distinct phases; each involving the substantial collection and/or processing of personally identifiable information. The first phase is the registration of PoCs, a process at the heart of all UNHCR operations, and applicable to all its assistance, not only CBIs. The second is the identification, targeting and assessment of potential beneficiaries of cash assistance. This can involve extensive data sharing with partners and various forms of eligibility assessment (i.e., for CBIs and other forms of assistance). The third phase is the disbursement of funds, which can include the creation of virtual bank accounts for beneficiaries, the distribution of ATM cards and the withdrawal of payments by refugees. The fourth phase is monitoring and evaluation, which involves various processes designed to assess the use and impact of cash assistance, satisfy auditing requirements and improve the methods employed in phases 2 and 3.

4.1 Registration

In the country operations examined by Trilateral, the basic information used to target and assess refugees for eligibility for cash assistance was derived from the data collected during the registration process. Registration serves numerous purposes. It provides refugees and asylum-seekers with UNHCR status and documentation, which can, in turn, protect them against refoulement, arrest or detention; it helps the UNHCR and its partners determine the resources needed to support refugee populations and identify those with special protection or assistance needs; and it supports family reunification and provides a basis for durable solutions (voluntary repatriation, local integration or resettlement). UNHCR conducts registration through an interview process used to gather and verify bio-data and other personal information from persons of concern.

The amount of data collected during registration varies depending upon local protection concerns and operational considerations. In the two countries examined by Trilateral, the data collection comprised extensive biographical data, political and religious affiliations, travel history, reasons for flight and/or the basis for asylum claim. Photographs and iris scans were also collected. All persons registered receive a unique individual identification number and a household or case identification number. Registered persons were also asked to consent to the sharing of their biographical data with humanitarian organisations for assistance purposes at the time of registration. The data collected at registration was stored in two databases: proGres (the universal UNHCR registration software) and a dedicated biometric identification system. Selected registration data was then exported to dedicated refugee assistance databases.

Depending on the requirements of the host governments, refugees may have to register with local authorities. UNHCR may also be under an obligation to share certain personal data elements on refugees and other persons of concern with the national authorities, and communicates any such requirements to those it registers.

4.2 Targeting and vulnerability assessment

UNHCR and its partners may also collect and share information about persons of concern and their circumstances in order to identify and assess the eligibility of specific households for cash and other forms of assistance. In the country operations where the two PIAs took place, UNHCR routinely provides contact and basic biographical data regarding refugees to humanitarian agencies operating assistance programmes. Data was supplied on digital media (including e-mail, CD-ROM and USB devices) or

[16] Note that information flows and data processing arrangements may differ across UNHCR's operations.

accessed directly from UNHCR hosted-databases.[17] In many cases, the recipients of UNHCR data retain, amend and, in some instances, further share the data, for example, within their own organisations or with their own local partners. UNHCR may in turn receive information back from its partners, including data collected during the eligibility assessments, the results of surveys and evaluations, and corrections or changes in refugee contact details and circumstances. It is important to stress the extent of the data-sharing and supplementary collection at this stage; many partners who receive an initial list of refugees eligible for the assistance programmes from UNHCR effectively establish their own database, whether in the form of a spreadsheet or dedicated content management systems.

In the two operations assessed, UNHCR determines whether refugees and PoCs are eligible to access its CBIs in several ways. It analyses the personal data gathered at registration to identify the most vulnerable categories of refugees (for example, female-headed households, separated or unaccompanied minors, persons with special needs, etc.), with additional home assessment visits used to derive additional information about refugee circumstances. By using proxy data to determine vulnerability in multiple areas, these surveys can significantly widen the amount and scope of the data collected from refugee households in order to target assistance. Econometricians have developed models for country operations that use a variety of indicators and a rule-based scoring system to ascertain different dimensions of vulnerability (i.e., what makes people more or less vulnerable, and in which ways, rather than simple assessments of whether someone is vulnerable or not). This reflects a desire on the part of UNHCR and its partners (and donors) to better understand the needs of refugee households and, on this basis, to better target and deliver assistance to those who need it most. This may be achieved by developing sector-wide assessments that can be used by the humanitarian community as a whole in place of the current ad hoc approaches to targeting.

Vulnerability assessment data may include information relating to refugees' financial situation, quality of housing, immigration and asylum status, employment, children's needs, food security, coping strategies, WASH (water, sanitation and hygiene), health, education, disability, legal situation and overall social and economic vulnerability. In addition to providing richer data, harmonised assessment methodologies used by multiple organisations providing assistance to PoCs can contribute to a reduction in "survey fatigue", caused by repeated assessments by different organisations, as partner agencies and humanitarian organisations – each of which have their own assessment methodology and data collection systems.

4.3 Cash distribution

Once UNHCR has determined that a refugee or household is eligible for cash assistance, it works with implementing partners to get the funds to the beneficiaries. Most modern CBIs involve financial service providers. In the two countries where the PIAs took place, the financial service providers provided UNHCR's account with sub-accounts, which were assigned to beneficiaries, and through which UNHCR could distribute cash assistance. Local partners may also be employed to distribute the ATM cards and PIN numbers. Once UNHCR has completed its internal checks and due diligence measures, it registers the beneficiary accounts with the bank, and provides a schedule of payments detailing the accounts to be credited and the value of each payment. When the banks process the deposits, UNHCR or the bank will notify the beneficiaries that the funds are available for withdrawal. Refugees receive additional information about how and where to use the different banking facilities during enrolment for or distribution of cash assistance, and helplines are available in case of problems. In countries with large-scale urban refugee populations, there may be dozens of INGOs operating small or large-scale CBIs, each with their own distribution modalities and partners. Groups of humanitarian organisations are now considering new ways of working together through common delivery mechanisms.

[17] Since the PIA, UNHCR has changed practices to include VPN in the operations subject to the PIA.

4.4 Monitoring and evaluation

UNHCR and its partners collect and retain further information regarding refugees and their use of cash assistance after the money has been distributed, in order to monitor the implementation, assess the impact and provide an audit trail for its CBIs. This process occurs in three main stages. First, financial partners monitor the usage of accounts and provide all transactional data to UNHCR, enabling the organisation to identify possible problems in distribution and to terminate inactive accounts. Second, agencies survey beneficiaries to assess the practical operation and impact of their cash assistance. This includes exit interviews, surveys of beneficiaries and qualitative impact assessments. Standardised Post Distribution Monitoring (PDM) questionnaires may be used to assess refugee experiences in accessing and using cash assistance. Third, UNHCR and its partners must retain data for auditing purposes. This includes hard copy and electronic data from across their operational programming, which may be retained indefinitely or for at least five years.

CONTENTS

5 Key findings

5.1 Privacy risks matrix

Privacy principle	Challenges facing UNHCR cash-based interventions
Consent and choice: presenting to the data subject the choice whether to allow the processing of their personally identifiable information (PII)	Refugees often have little real choice but to register with UNHCR and to consent to subsequent data sharing if they want to access CBIs and other forms of assistance. The challenge is therefore to ensure that refugees are properly informed about how their data will be used and for what purposes, and to allow them to withdraw their consent at any stage.
Purpose legitimacy and specification: ensuring that the purpose of data collection is specified and lawful	In developing CBIs, UNHCR may use registration data for purposes other than that for which it was collected, and risks function creep if data collected specifically for cash assistance is later used for a purpose not specified to the PoC at the time of collection. Partners may also use UNHCR refugee data for purposes other than stated at the time of exchange (e.g., an NGO or financial partner uses data for unrelated programme or commercial purposes).
Collection limitation: limiting the collection of PII to that which is within applicable law and strictly necessary for the specified purpose(s)	The targeting and eligibility assessments used to identify the most vulnerable refugees for inclusion in CBIs can increase the amount of sensitive data collected by UNHCR and its partners and result in the profiling of refugee households. There is a risk that more data is collected than necessary in the drive to better understand vulnerability. This also poses novel challenges in terms of protecting and sharing these datasets with partners. There is a consequential risk of partners using this data for purposes other than those for which it was originally collected and shared.
Data minimisation: minimising the PII processed and the number of privacy stakeholders to whom PII is disclosed or who have access to it	All of the above risks are compounded if too many people have access to refugee PII, both within UNHCR and partner organisations.
Retention and deletion: ensuring that data is not kept for longer than is necessary for the purpose specified	UNHCR and other humanitarian agencies are bound by strict auditing requirements imposed by donors, leading to their retaining data indefinitely. This amplifies the privacy risks to refugees.
Accuracy and quality: ensuring that the PII processed is accurate, complete, up to date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use	The collection and sharing of data across CBIs has resulted in the creation of multiple databases containing personal information within UNHCR and partner organisations. There is a risk that inaccurate or obsolete data is contained is some datasets, or that outdated information is retained unnecessarily.

Privacy principle	Challenges facing UNHCR cash-based interventions
Openness, transparency and notice: providing data subjects with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to processing of PII	In the context of multiple CBIs operated by multiple agencies, there is a significant risk that refugees are unable to grasp how their data is being used, with whom it will be shared, and for what purposes. It may in practice be very difficult to even understand who the data controller is, what their policies are, or which organisation is taking decisions about their eligibility for assistance.
Individual participation and access: giving data subjects the ability to access and review their PII, provided their identity is first authenticated (Access and correction)	In the absence of clear information about how data is used, refugees are unable to exercise their rights control over their personal data. There is a legitimate need for cash assistance providers to withhold some information concerning eligibility determination to prevent attempts to unscrupulously access assistance using deceit or deception, but subject access rights must be extended as far as possible to all data subjects.
Accountability: assigning to a specified individual within the organisation the task of implementing the privacy-related policies, procedures and practices	At the time of the PIAs, UNHCR had not yet adopted its global data protection policy, and responsibilities were shared and addressed on an ad hoc basis by country operations with limited guidance from HQ. The implementation of the new UNHCR global data protection policy provides the opportunity to increase accountability for refugee privacy in all operations.
Information security: protecting PII under an organisation's control with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and to protect it against risks such as unauthorised access, destruction, use, modification, disclosure or loss.	UNHCR registration protocols and the proGres database application provide in-country operations with relatively robust and secure systems. However, the export of data from proGres and the creation of supplementary refugee assistance databases undermine this architecture if too much data is extracted and exchanged, or if the exported data is not subject to the same level of information security. The challenge of making refugee data available for assistance purposes while ensuring a high level of data protection reaches far beyond cash assistance to other areas of assistance.
Privacy compliance: verifying and demonstrating that the processing of data meets data protection and privacy legislation by periodically conducting audits using internal or trusted third-parties	Audits of CBIs focus strongly on anti-fraud and donor compliance measures, with little emphasis on refugee privacy. To minimise risks to refugee privacy, all CBIs should ensure that data processing meets international standards.
Data transfers: do not store or transfer personal data to third parties without adequate assurances that they will safeguard it to a standard comparable to that of the UNHCR.	CBIs and other assistance programmes pose inherent risks that data is transferred to partner organisations with minimal oversight or adherence to data protection policies. Data may be transferred insecurely (on USB sticks, CD-ROMs, in unencrypted e-mails, etc.), stored by partner organisations on external devices, backed up in e-mail inboxes, saved on individual desktops, imported into new databases, etc.

5.2 Threat and vulnerability matrix

Threat	Vulnerability	Risk	Mitigation
Cyber espionage	Governments and non-state actors have not developed capabilities to repel cyber intrusions	UNHCR systems hacked by 3rd party with malevolent intent	Improve information security; improve data protection policy
Physical loss of data	Multiple people carrying around external devices with refugee data	UNHCR staff lose data storage devices such as a laptop or a memory stick.	Centralise data rather than transferring/ sharing on portable media
Technical failure	Infrequent back-ups, inadequate protections against power loss or hardware failure.	UNHCR information systems fail	Implement data back-up and recovery methods. Develop and implement disaster recovery plan.
Unauthorised acquisition -- Governments in countries of refugees' origins are keen to acquire refugee data, which is of a highly sensitive nature. Many governments are interested in refugee data for counter-terrorism purposes.	UNHCR and its partners have not developed policies and procedures to respond to governmental requests for data.	An unauthorised organisation acquires personal data from UNHCR and/or other partners	Improved information security based upon a thorough information security audit and implementation of its recommendations; assurance of data security with partners through data sharing agreements and data user training
DDOS attack / malware	Inadequate updates to network security systems and/or optimised security infrastructure.	UNHCR systems taken down	Execute and implement results of information security audit.

Insider privilege abuse	Staff corruption (e.g., bribery)	UNHCR staff or partner organisations sell refugees' PII.	Vet staff carefully, maintain log files, restrict access to databases
Partner abuse – Partners might use UNHCR refugee data for unauthorised purposes	UNHCR does not have procedures in place to check how partners use the PII it shares.	3rd party uses UNHCR data for purposes other than for which it was acquired.	Tighten data sharing policies and strict enforcement of purpose limitation; Implement data audits
Partner negligence – A partner may undermine refugee privacy and data protection; the bank makes mistakes in relation to distribution; the bank passes data to third party provider of due diligence/ compliance services.	The bank does not have adequate checks and controls on cash distribution.	The bank does not distribute cash to some of those who are legitimately eligible. A partner organisation loses refugee data.	Tighten data sharing policies and agreements. Insist on audits. Enforce strict purpose limitation. Seek clarification on the circumstances in which the bank would share data with third parties, whether named refugees are vetted against counter-terrorism and other sanctions lists, and if third parties are involved.
Refugee complaints and litigation	Refugees are unhappy with how their data is collected, used or transferred; Refugees are unhappy at their treatment at the hands of a UNHCR partner (e.g., a bank or supermarket)	A refugee complains to a human rights advocacy organisation or IGO about the misuse of their data leading to reputation damage.	Implement transparent processes around information collection, purpose specification, processing and transfer. Revise informed consent procedures and subject access policies.
Reputational damage	Above risks materialise	UNHCR's trust and credibility undermined because of data protection failures	Implement mitigation measures

5.3 Operational assessment

UNHCR has developed pioneering unconditional CBIs, involving multiple partners, and overcoming complex distribution issues. Due to the complex nature of the relationships between UNHCR and partner organisations, and the range of needs and requirements of all parties involved, data collected from refugees has increased substantially as CBIs have developed. This highlights a host of existing privacy and data protection risks for UNHCR as the data controller. Should the humanitarian community continue to scale up their cash interventions, the pressure on UNHCR to share refugee data is likely to increase in the future, potentially amplifying these risks.

Refugees may harbour fears about how their personal data is used, including by host governments. Some refugees choose not to register with UNHCR, though the reasons for this are many and varied. It is acknowledged that refugees have little real choice but to consent to the processing of their data if they wish to register with UNHCR and avail themselves of the benefits this status brings. Similarly, it is obviously in their interest to consent to the sharing of their data to access the assistance programmes of other humanitarian organisations. But this should still be an informed choice, and refugees should be made aware of how their data will be used to the fullest extent possible.

The Trilateral PIAs found room for improvement in the process by which refugees' informed consent is obtained, and opportunities to improve the information provided to refugees about how their data will be used, what sort of assistance they may be eligible for, and how to obtain redress. In particular, while UNHCR procedures allow refugees to request access to information held about them, there was no clear policy in place at the time of the PIA setting out how this can be done or what kind of data can be provided and withheld. Although there may be legitimate reasons for withholding certain information, for example, about status determination or programmatic eligibility, data controllers should seek to grant the widest possible access to information to data subjects.

UNHCR is to be commended for the flexibility it has demonstrated in developing the information systems required to support and enhance its CBIs. Nevertheless, there are concerns about the breadth of access to UNHCR data necessitated by multi-stakeholder cash assistance and the insecure manner in which data has been shared in certain instances. Whereas the proGres database application provides in-country operations with relatively robust and secure registration databases, the export of biographical and other personal data from proGres into ad hoc refugee assistance databases operated by UNHCR and its partners poses numerous data protection and information security challenges.

With no centralised refugee assistance application available to use, and in the absence of established global policies regarding the establishment of such information systems, UNHCR regional and in-country operations have, in the past, gradually improved information security around these refugee assistance and cash distribution databases on an ad hoc basis. As with all UNHCR activities, the technical infrastructure of in-country operations is highly resource-constrained and much depends on the initiative of data and IT managers. In both country operations assessed, Trilateral found that these staff had instigated commendable data protection and information security measures in the absence of central guidance or standard operating procedures. This included secure methods for distributing ATM cards to their intended recipients and enhanced security and external access controls around refugee assistance databases.

While it is preferable for UNHCR to retain control over the refugee data it shares by making the data available to partners through secure databases, the absence of established data processing solutions for CBIs and related programmes, and problems with telecommunications connectivity, mean that it is inevitable that in-country operations will have to find innovative means of sharing large datasets during humanitarian crises. These transfers should nevertheless implement high levels

of data security. As the initial data controller, UNHCR also bears significant responsibility for what its partners do with the PII it shares. While the UNHCR data sharing agreements examined for the PIA contained adequate safeguards in principle, there is a need to strengthen procedures for developing and authorising these agreements, and to implement controls and audit mechanisms to monitor adherence to those agreements. This includes checks as to the adequacy of partner data protection policies prior to the signing of data-sharing agreements and guidance as to how partners should meet the requirements therein. These safeguards are necessary to enforce the core principles of data protection in relation to data sharing: purpose limitation, disclosure limitation (the prohibition of onward sharing), accuracy and quality (deletion of spurious or redundant datasets). In the absence of these mechanisms, bad practice and data breaches risk going undetected.

The supplementary collection of data on refugee households by UNHCR and its partners increases significantly with large-scale CBIs, posing significant challenges in terms of refugee data privacy. Enhanced data collection and analysis techniques have the potential to better understand the needs of PoCs and greatly improve the delivery of assistance to them. However, the corresponding requirement for ever more detailed household assessments is encouraging function and scope creep. Robust privacy and data protection policies should guide future decisions about the use of refugee data across the humanitarian sector.

The involvement of commercial financial institutions in the distribution of cash assistance poses additional privacy challenges. Trilateral commended UNHCR's CBIs for their innovative and secure approaches to cash distribution implemented in partnership with financial service providers. Confidentiality agreements between UNHCR and financial partners appeared robust and ostensibly prevent the banks from sharing refugee data with any third party, including the host governments. However, all commercial banking services must act in accordance with national and international regulations and meet their obligations in regard to co-operation with financial investigations and due diligence in combatting money laundering and the financing of terrorism, which requires account holders to be checked against multiple sanctions lists, and transactional data to be retained for law enforcement purposes. The CBIs that Trilateral examined provided refugees with 'virtual' UNHCR accounts which may be exempt from such checks. However, Trilateral was not able to clarify the circumstances under which data could be shared with the external authorities. Given the transnational reach of national counter-terrorism efforts, this issue has important implications for refugees.

5.4 Sector wide issues

The need to quickly establish field operations and assistance programmes capable of meeting urgent humanitarian needs of hundreds of thousands of people is incredibly challenging. The need to reach vulnerable persons, deliver assistance and achieve efficiencies in a crisis situation – coupled with the rapid pace of innovation in cash assistance, divergences in approach among different organisations and stakeholders, and the rigid mandates and division of responsibilities among UN agencies – compounds these problems.

Although the CaLP guidance on privacy and data protection is relatively new (November 2013), there has been little in the way of concerted attempts to mainstream the guidance across the cash sector in the countries Trilateral visited, for example, in the in-country, multi-stakeholder 'Cash Working Groups'. This is not to say that there was no concern or attention to these issues, just that they had been dealt with on a more ad hoc basis. Trilateral also found that within many of the organisations interviewed during the course of the PIAs, staff lacked basic knowledge, training and awareness about their corporate data protection or information security policies. Some organisations did have high standards, but there was a clear need to enhance privacy protection across all actors implementing CBIs.

One of the major tensions identified during the course of the PIAs is the competing requirements for UNHCR and its partners to protect refugee privacy while simultaneously being compelled to retain extensive data about refugees and cash assistance for auditing purposes. The deletion of personal data that is no longer necessary for the completion of a specific task is a core principle of data protection, but in the absence of policy to the contrary, UNHCR and its partners are keeping masses of refugee data indefinitely to satisfy future audit requirements. All of the organisations to whom Trilateral spoke in the course of the PIAs retain personal data about refugees for at least five years or in some cases indefinitely in the absence of any substantive guidance on safeguarding such datasets, minimising or anonymising them, or deleting spurious information. Keeping data that is no longer needed, retaining data for excessively long periods, and making it available internationally to programme managers and auditors inside and outside of the organisation, unnecessarily jeopardises refugee privacy. Audit processes should be as concerned with the protection of personal data as tracing the use of funds.

The international donors and supporters of CBIs, including the European Union, have a role to play in mainstreaming good practice across actors implementing CBIs. They are encouraging the harmonisation of targeting and distribution methods and the deployment of econometric targeting techniques – which can substantially increase the amount of data collected about vulnerable persons – but as yet have not placed a corresponding emphasis on privacy and high levels of data protection.

6 Recommendations

It is important to stress that it is not the collection and processing of personal information for cash assistance purposes that is problematic per se – UNHCR is clearly using the data for entirely legitimate purposes with clear benefits for those they support. The overarching challenge is to minimise the amount of data that is collected, exchanged, stored and accessed at every level of UNHCR's overall programme design and implementation. The recommendations that follow are divided between UNHCR's corporate-level and in-country operations. Where they have appropriate competencies, regional UNHCR offices should also be involved in the implementation of the recommendations. The implementation of the newly agreed UNHCR data protection policy is the foundation from which to address these recommendations.

6.1 Corporate level

Recommendation 1: Strengthen data protection mandates and improve oversight of refugee data processing in country operations. The successful implementation of UNHCR's new global policy rests on adequate understanding, prioritisation, training, experience and resources being made available to in-country offices to implement data protection policies and improve information security measures in order to better protect refugee privacy.

Recommendation 2: Include targeting, assessment and cash assistance modules in proGres 4 – or develop refugee assistance databases that can be rolled out globally. Adequate functionality, fully addressing the requirements of and lessons learned from CBIs, should be built into proGres 4 (the next iteration of the global UNHCR registration database). Alternatively, resources should be invested in robust systems already developed in the field to allow them to be rolled out elsewhere. In either case, UNHCR should ensure that any new refugee assistance systems follow the principles of privacy by design in order to mitigate privacy and data protection risks before the new systems are rolled out.[18]

[18] Kroener, Inga, and David Wright, "A strategy for operationalising privacy by design", The Information Society, Vol. 30, No. 5, 2014, pp. 355-365. Cavoukian, Ann, Seven Foundational Principles of Privacy by Design. www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/.

Recommendation 3: Develop and roll out good privacy and data protection practices for CBIs. Although there is a great deal of variation regionally with respect to CBIs, UNHCR should provide guidance to field offices that will enable them to make use of the knowledge gained in this area to date. This guidance should include SOPs for implementing CBIs (taking into account the potential for geographic and social differences, local IT infrastructure, differing partners, jurisdictions, etc.) and privacy and data protection standards that promote best practices.

Recommendation 4: Work with other UN organisations, donors and INGOs to establish minimum standards for data minimisation and protection in regard to CBIs. Given the rapid expansion of cash assistance among humanitarian organisations, UNHCR should work with key stakeholders to develop a set of minimum standards for data retention and storage vis-à-vis the extensive data collected during the course of such operations with a view to minimising and anonymising data as far as possible. Particular emphasis should be placed on minimising the amount of PII that is kept for audit purposes.

Recommendation 5: Appoint a Data Protection Officer (DPO) with a mandate that reflects the changing use and increased sharing of UNHCR data. The post of DPO should be established independently of (but working constructively with) existing registration, programming and operational staff to ensure that refugee privacy and data protection are properly represented in discussions about the use and sharing of personal information. At a minimum, the mandate for the DPO should include at least the following responsibilities:

1 ensuring that minimum standards for refugee privacy and data protection are upheld in all UNHCR data processing activities;

2 ensuring that any new proposed uses of personal data are necessary, proportionate and respectful of refugee privacy rights;

3 developing, in conjunction with senior management from relevant divisions, a data protection plan that comprehensively addresses the concerns raised in this report and the obligations arising from UNHCR's new global policy (the plan should include a review of all existing data processing activities with a view to minimising, limiting and anonymising the processing and sharing of data as far as possible, and should codify the relevant best practice developed by UNHCR staff and its ICT specialists in minimum standards to be followed across the organisation);

4 improving and authorising data sharing agreements with third parties (see further Recommendation 11, below) and reviewing their implementation;

5 reviewing the development and implementation of UNHCR's use of biometric identification systems to ensure compliance with best practice;

6 developing and implementing a training programme focusing on data protection and privacy for all UNHCR staff, as well as partner organisations (training programmes can be run online or in person);

7 developing and overseeing the implementation of a subject access request policy covering all data processing operations (see further Recommendation 14, below);

8 developing and implementing a policy for identifying, investigating and responding authoritatively to data breaches;

9 promoting the development and implementation of data protection standards in regional offices as well as at headquarters; and

10 developing a wider "privacy culture" within the organisation.

6.2 Country level

Recommendation 6: Revise SOPs and other relevant guidance to include minimum standards for data protection. In conjunction with relevant departments, the newly appointed DPO should review all current SOPs that have a data processing element to ensure that due regard is paid to refugee privacy and data protection at each and every stage of the operation. UNHCR in-country operations should also ensure that the terms of reference for Cash Working Groups (comprising multiple organisations operating CBIs) include a commitment on the part of all participants to implement the minimum standards for refugee privacy protection adopted by CaLP into their programming (see section 3, above); to collectively address any privacy-related matters arising from new technologies or practices; and to share best practice on data protection and refugee privacy issues.

Recommendation 7: Conduct an information security audit of refugee assistance databases. The information security audit should examine physical, logical and network security. It should evaluate existing access controls and provide a detailed report with recommendations for correcting identified information security flaws.

Recommendation 8: Conduct a third-party evaluation of local and regional biometric identification systems. As noted in section 3.2.2, above, the collection of biometric information requires additional privacy and data protection safeguards due to the sensitive nature of the data. Biometric information can potentially allow a greater level of surveillance and tracking than that which is possible with other personal data. The risks are multiplied when biometric databases become "multimodal" (i.e., several different biometrics are collected and stored in one database and combined with traditional data points such as name, address, date of birth). The evaluations should address information security and measures to mitigate against secondary uses of biometric data held in UNHCR databases.

Recommendation 9: Review the impact of the implementation of new vulnerability assessment frameworks on refugee privacy and data protection after 18 months of operation. Where UNHCR country operations employ novel vulnerability assessment methodologies based on comprehensive household surveys, these frameworks should be reviewed using CaLP privacy standards as a baseline. The objective should be to minimise the amount of personal data captured by home visits and stored in refugee assistance databases, to ensure the legitimacy and effectiveness of data profiling and targeting operations, and to review information sharing and access controls.

Recommendation 10: Develop ICT policy and procedures. Gaps in ICT governance should be addressed in a comprehensive ICT policy and procedures document that includes roles and responsibilities, systems and data security policies, data use and retention policies, disaster recovery and systems redundancy procedures and data breach policy and procedures.

Recommendation 11: Implement a program of governance for data sharing. Though robust procedures exist to ensure that the sharing of data with third parties is governed by an appropriate agreement or MoU, they are implemented inconsistently. In-country operations should develop a holistic approach to working with third parties on data sharing by instituting a program of governance that (1) sets policies and standards for data-sharing; (2) develops clear and consistent language for data use; (3) establishes clear SOPs for entering into data-sharing agreements; (4) conducts audits to ensure compliance with policies and standards; and (5) provides the support required to enable third parties to comply with their obligations. Specifically, the SOPs should include a "safe harbour" process (in which third parties demonstrate that they have appropriate minimum standards for data protection in place within their own organisations before such an agreement is concluded) and a minimisation review, to ensure that data sharing has been limited to the minimum amount necessary.

Recommendation 12: Review data sharing arrangements with financial partners. UNHCR in-country operations should seek clarification from financial partners as to the circumstances in which they would provide refugee data to the Central Bank or government authorities, whether data is kept for auditing purposes and if so for how long; whether named refugees are vetted against counter-terrorism and other sanctions lists; and if third parties are engaged in the performance of such due diligence.

Recommendation 13: Improve data sharing practices. UNHCR operations should also develop a set of minimum standards for external data transfers. The transfer of refugees' personally identifiable data in unencrypted files and on media susceptible to loss or theft should be restricted to an absolute minimum. Where possible, the practice of e-mailing such files should be replaced with secure FTP channels or VPNs.[19] If files are to be e-mailed, the practice of transmitting encrypted files and the passwords and for those files in successive e-mails should also cease in favour of a more secure procedure. The medium-term objective should be the implementation of secure ICT solutions that allow partners to access and use UNHCR data (and correct or augment where necessary), but through which UNHCR retains much greater control of data on PoCs.

Recommendation 14: Revise informed consent procedures. In a situation in which refugees have little choice but to consent to the processing and sharing of their data in good faith that this will render them assistance from the UN or its partners, UNHCR should ensure that informed consent procedures provide as much relevant information to refugees as possible. Such consent should be sought and expressly given prior to any data collection exercise, whether as part of a registration procedure, an assessment or post-distribution monitoring exercise. In each case, the informed consent process should include a clear explanation as to why the data is being collected, the purposes for which it will be used, organisations with which that data may be shared (including financial institutions and government agencies), and the reasons for such exchanges. In each case, this verbal explanation should be backed up with an information sheet to be given to the data subject that contains the same basic information and describes the basic principles and measures that UNHCR has in place to protect refugee data.

Recommendation 15: Introduce procedures to facilitate and respond to subject access requests. UNHCR should prioritise the introduction of an appropriate subject access policy comprising a dedicated contact point (usually the DPO), information to subjects on how and where to submit their requests, SOPs for handling such requests, the envisaged maximum time frame for responding to requests, and any further information that affects their rights. For example, if UNHCR envisages withholding data in response to subject access requests – and there may be legitimate operational or procedural reasons for doing so – it should qualify the scope of those restrictions and establish an appeals procedure involving an appropriate oversight body. UNHCR should provide information about subject access procedures during the informed consent process and on the information sheet envisaged in the previous recommendation.

[19] UNHCR has already implemented some of these recommendations, such as this one on improved processes for file transfer using FTP channels and VPNs. It has also adopted a policy on data protection.

This material was developed as part of the European Commission Humanitarian Aid and Civil Protection Department's Enhanced Response Capacity funding (2014–15).

This inter-agency project was led by the Office of the United Nations High Commissioner for Refugees on behalf of its partners: the Cash Learning Partnership, Danish Refugee Council, International Rescue Committee, Norwegian Refugee Council, Save the Children, Oxfam, United Nations Office for the Coordination of Humanitarian Affairs, Women's Refugee Commission, World Food Programme, and World Vision International.

Humanitarian Aid
and Civil Protection