United Nations University
Centre for Policy Research

WORKINGPAPER

November 2023

Global Data Sharing Arrangements between UNHCR and other UN entities and International Organizations

Alex Novikau, Chief Data Protection Officer, UNHCR

Dogu Han Buyukyagcioglu, Data Protection Officer, UNHCR

This paper was presented at a joint expert event co-convened by UNU-CPR and the International Chamber of Commerce on 8 November 2023 in New York.

Introduction

Use of data in a humanitarian context is essential for life-saving interventions and the successful execution of programmes during crises. For instance, timely and accurate prediction of forced displacement trends[1] allows all entities that are responding to a humanitarian crisis to make informed decisions relating to the allocation of resources, the establishment of tailored processes, and advocacy for protection and solutions. Accurate data on nutritional status can guide the distribution of food and therapeutic supplies to prevent malnutrition. Information about the spread of contagious diseases in a refugee camp can direct medical aid to where it is needed most urgently, potentially curbing an epidemic. Knowing the age, gender, and diversity profile of the population can assist in the design of education programmes and health services. Data on security incidents within a displacement setting can lead to targeted protection measures and advocacy for better safety provisions. All these examples underline the profound importance of precise data collection and analysis in ensuring that aid is both efficient and effective.

Having mutual commitments among humanitarian actors regarding data collection, usage, and sharing can streamline its transparent and effective use of data, provided they account for specific contexts. When these commitments encompass the processing of personal data, they must adhere to data protection principles and standards. However, translating these commitments into action can be challenging. The required technical know-how and infrastructure to facilitate such solutions aside, there are legal and ethical frameworks that must be considered. The 'do no harm' principle, for example, mandates entities to avert any adverse impact on affected communities.

Especially in the context of humanitarian work, such data often includes or derives from personal data of those affected by crises. This requires careful attention for many reasons.

To begin with, protection of such personal data is an integral part of protecting individuals' life, integrity, and dignity in a humanitarian context.[2] And for the United Nations High Commissioner for Refugees (UNHCR), data protection is part and parcel of refugee protection.[3] For forcibly displaced and stateless persons, misuse or unauthorized disclosure of their personal data could result in far greater negative impacts, and lead not only to identity theft and fraud but also discrimination, stigmatization, and even violence or persecution.

Similarly, the likelihood of such risks materializing could also be higher given their particular and vulnerable situation. Processes that are set up without taking into account the context of a particular situation, and that lack safeguards to center the agency of the individuals whose personal data collected, used and shared, are prone to result in function creep and misuse of

[1] For UNHCR's initiative on Nowcasting, See, Andrea Pellandra and Giulia Del Panta, "The Power of Now: Nowcasting Refugee Population Figures at UNHCR," 10 February 2023, *UNHCR Blogs,* https://www.unhcr.org/blogs/the-power-of-now-nowcasting-refugee-population-figures-at-unhcr/.
[2] ICRC, *Handbook on data protection in humanitarian action, Second Edition*. Accessible at: https://www.icrc.org/en/data-protection-humanitarian-action-handbook.
[3] See, Alexander Beck, "Data protection is part and parcel of refugee protection," 23 May 2018, *UNHCR Blogs,* https://www.unhcr.org/blogs/data-protection-part-parcel-refugee-protection/.

personal data. In view of this, even data elements not typically deemed to be among special categories of personal data[4] take on heightened sensitivity in humanitarian contexts.

Finally, UNHCR is entrusted with particularly sensitive personal data of refugees, asylum seekers, internally displaced persons (IDPs), stateless persons, and returnees. Any misuse or overreach in using such data could erode trust from these groups and the global community, hampering UNHCR's mission.

This article examines the implementation of UNHCR's global data-sharing arrangements with other UN agencies and International Organizations, which aim to facilitate transparent and efficient personal data sharing while adhering to relevant principles and standards.

While doing so, it will also touch upon the particular context in which such arrangements are being created and implemented, the applicable frameworks, and the issues such arrangements aim to address.

The Context

UNHCR is a global organization dedicated to saving lives, protecting rights, and building a better future for people forced to flee their homes because of conflict and persecution.

UNHCR was established by the United Nations General Assembly in 1950 and is mandated by Member States to assume the function of providing international protection, and together with Member States, to facilitate solutions for forcibly displaced and stateless persons.[5]

At the end of 2022, there were 108.4 million people forcibly displaced as a result of persecution, conflict, violence, human rights violations, or events that seriously disturbed public order. This figure encompasses refugees (including refugees who are not covered by UNHCR's mandate), asylum-seekers, internally displaced persons, and other people in need of international protection.[6] Notably, 76 per cent of these individuals reside in low- to middle-income nations, with 70 per cent being housed in nations neighboring their countries or origin.

UNHCR operates in 137 countries with 476 field offices, and works with nearly 900 partners, including NGOs, international NGOs, other UN entities, international organizations and governments.

This results in complex global data flows which are essential to effectively deliver protection, assistance, and solutions to forcibly displaced and stateless persons. The data flows are diverse and at a global scale, and they occur in countries where there are well-established legislative frameworks for data protection, as well as those where such frameworks are limited or non-existent.

[4] For instance, see, Regulation (EU) 2016/679 - General Data Protection Regulation, Article 9.
[5] For further details on UNHCR's mandate, See, UN High Commissioner for Refugees (UNHCR), *Note on the Mandate of the High Commissioner for Refugees and his Office* (October 2013). Accessible at: https://www.refworld.org/docid/5268c9474.html.
[6] See, UN High Commissioner for Refugees (UNHCR), *Global Trends Forced Displacement in 2022* (June 2023). Accessible at: https://www.unhcr.org/sites/default/files/2023-06/global-trends-report-2022.pdf.

UN entities are accorded with privileges and immunities by Member States to allow for the independent and effective exercise of their functions and mandated activities, and thus national data protection frameworks are not enforceable on UN entities. Nevertheless, operating across multiple jurisdictions adds another level of complexity, since UN entities and International Organizations often work in collaboration with local partners or governments. The scope of this paper is the arrangements between UNHCR and other entities which have privileges and immunities, and such complexity will therefore not be elaborated.[7]

Having said that, UN entities and International Organizations do not act in vacuum when it comes to processing and sharing personal data. They act in line with their own data protection and privacy frameworks that are applicable to them wherever they operate. In the context of UNHCR, this is the personal data protection and privacy framework established by the General Policy on Personal Data Protection and Privacy, adopted by the High Commissioner.[8] The requirement of such a framework informs the structure and requirements of UNHCR's data-sharing arrangements with third parties.

The Framework

UNHCR adopted its Policy on the Protection of Personal Data of Persons of Concern to UNHCR in 2015, establishing UNHCR's data protection principles. It is a High Commissioner's Policy (HCP), for which compliance is mandatory for all staff.

In 2018, the UN High-Level Committee on Management (HLCM) adopted the Personal Data Protection and Privacy Principles which set out a basic framework for the processing of 'personal data,' defined as information relating to an identified or identifiable natural person ('data subject'), by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.[9] These are considered to be high-level principles which inform frameworks that are adopted by each agencies. On their own, they represent the common denominators between different UN entities when it comes to personal data protection and privacy principles. In practice, they are built upon and elaborated by the respective data protection frameworks of each UN agency. UNHCR is not the only UN entity or International Organization with a dedicated personal data protection and privacy policy.[10]

[7] For an elaborated analysis of interplay between frameworks of International Organizations and domestic legislations, see Massimo Marelli, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", *Computer Law and Security Review* Vol. 50 (2023).
[8] UN High Commissioner for Refugees (UNHCR), *General Policy on Personal Data Protection and Privacy* (2022). Accessible at: https://www.refworld.org/docid/63d3bdf94.html.
[9] UN High-Level Committee on Management (HLCM), *Personal Data Protection and Privacy Principles* (2018). Accessible at: https://archives.un.org/sites/archives.un.org/files/_un-principles-on-_personal-data-protection-privacy-hlcm-2018.pdf.
[10] For other examples, see ICRC, *ICRC Rules on Personal Data Protection* (Geneva, 2020). Accessible at: https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection; "UNICEF Policy on Personal Data Protection," UNICEF, 15 June 2020, https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf ; "World Bank Group Policy, Personal Data Privacy," World Bank Group, 1 February 2021, https://ppfdocuments.azureedge.net/0298ff3b-8893-4894-91af-1ffb7c0d59e1.pdf; "WFP Guide to Personal Data Protection and Privacy," World Food Programme, June 2016, https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

UNHCR's latest policy, the General Policy on Personal Data Protection and Privacy (GDPP) was adopted in 2022 as an HCP. It brings the UNHCR's longstanding human rights-based approach to data protection and privacy in line with modern and global standards in this area.

The GDPP establishes the notion of UNHCR's data protection standards, which includes data protection principles, the rights of data subjects, and a set of operational standards. The latter includes a set of operational rules and requirements. These include the consideration of data protection and privacy by design and by default in the development of tools, systems, and processes that involve processing of personal data, the requirement of data protection impact assessments for processing operations that are likely to involve high risks to the fundamental rights and freedoms of data subjects, certain safeguards, and limitations to the use of automated decision-making and processing of sensitive personal data.

Under the GDPP, UNHCR's transfer of personal data with third parties is subject to two general conditions.

The first condition is that the transfer should be in line with UNHCR's data protection and privacy principles, should respect the rights of data subjects, and conform to UNHCR's operational standards. Transfer of personal data is a form of processing in its own right, and therefore needs to be in line with the applicable framework, which is the GDPP.

The second condition is that the transfer is executed based on arrangements that afford an adequate level of protection of personal data, as provided under the GDPP. The focus here is on the practical consequences of sharing personal data: UNHCR's data protection and privacy framework does not *ipso facto* apply to third parties, and therefore, when UNHCR transfers personal data to third parties, such personal data no longer benefits from the protection of UNHCR's data protection and privacy framework. Therefore, thorough assessment of the recipient party becomes crucial, and implementation of appropriate technical, organizational, and contractual safeguards for the transfer are necessary.

These conditions require tailored data-sharing arrangements which take into account the nature, scope, and objective of the transfer each time UNHCR makes a transfer of personal data to a third party. Using pre-determined transfer arrangements becomes impossible since they lack specificity and do not meet the requirements of UNHCR's framework.

This raises a practical dilemma between the need for timely and efficient sharing of personal data to enable implementation of UNHCR's mandate, and a requirement for establishing implementing arrangements that are particular to the circumstances and the data protection risks presented by each transfer.

This is where global data sharing arrangements prove their usefulness and relevance.

Global data sharing arrangements

UNHCR has established global level data sharing arrangements with a number of UN entities and International Organizations,[11] such as the World Food Programme (2018), the International Committee of the Red Cross (2021), and the World Bank (2023).

These global level arrangements share similar objectives, a coherent architecture, and due process guarantees. They are global level commitments that guide implementation at the field level. They aim to simplify and clarify the sharing of personal data on the ground. In so doing, they provide a level of predictability that is necessary for collaboration while ensuring that the principles set out by the data protection frameworks of each entity are respected. Moreover, they aim to safeguard the rights of data subjects, and to prevent the misuse of their personal data.

These data sharing arrangements usually consist of two components: A framework arrangement that is signed at the global level complemented by an implementing arrangement that can be further tailored and completed at the field level. Once the local implementing arrangement is in place, it forms a complete agreement for the specified geographical scope and comes into force alongside the terms and conditions of the framework arrangement.

These global level data sharing arrangements address five pivotal challenges, ensuring both efficient mandate execution and framework compliance:

Achieving adequate level of safeguards for protection of the shared personal data. The global level arrangements include a commitment relating to appropriate technical and organizational safeguards that are included in the framework arrangement agreed at the global level. These pre-defined safeguards are then complemented, as deemed necessary, at the field level with due regard to the particular operational context and reflected in the implementing arrangement. These may include contextualized incident response plans, or defined locations of processing operations.

The second issue is related to the *specification of purposes,* for which shared personal data is going to be processed by each entity. The framework arrangements come with broadly-defined objectives, namely the 'use-cases' that are pre-agreed by the parties. These use-cases are then further specified by the implementing arrangement, in accordance with operational needs. This aims to achieve the required level of local configurability at the operational level and compliance with the principle of purpose specification.

The agreed level of technical and organizational safeguards, and pre-determined use- cases, contributes to the predictable, *timely and effective implementation of programmes* by the respective entities. Operations can easily adopt the necessary contractual safeguards to start the implementation.

The global data-sharing arrangements provide *a degree of transparency and thereby agency to the individuals* whose personal data is being processed and shared. The requirements, which are

[11] One example that is publicly available is one with the World Food Programme. See UN High Commissioner for Refugees (UNHCR), *Addendum on Data Sharing to the January 2011 Memorandum of Understanding between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP)* (2018). Accessible at: https://www.refworld.org/docid/5bbcac014.html.

embedded into the global arrangement by design, includes provision of sufficient information to the individuals in a manner and language that is intelligible and makes available due processes for their exercise of rights as data subjects.

C*onsistency in application of other data protection principles* such as necessity and proportionality, retention limitation, and accuracy. The structure of the implementing arrangements prompts the end-users, who are the colleagues in charge of decision-making with respect to processing and sharing of personal data, to take into account these principles and thereby achieve compliance with the applicable frameworks of the agencies.

In conclusion, UNHCR's Data Transformation Strategy anticipates that data on forcibly displaced and stateless populations is critical to inform the international agenda and political debate on forced displacement and related issues, and to guide strategy development, policymaking, and programming choices at the global, regional, and national levels. UNHCR is well positioned to be a trusted leader on data and information related to refugees and other affected populations, thereby enabling actions that protect, include, and empower.[12]

Having high-level commitments by entities that are engaged in humanitarian work may facilitate data flows in practice. When such commitments involve collection, use, and sharing of personal data, it is critical that they allow a degree of configurability and specification which is required for compliance with data protection and privacy frameworks, and for tailored implementation with due regards to the operational contexts.

[12] UN High Commissioner for Refugees, *Data Transformation Strategy 2020-2025: Supporting Protection and Solutions* (2019). Accessible at: https://www.unhcr.org/media/data-transformation-strategy-2020-2025.

United Nations University
Centre for Policy Research

United Nations University - Centre for Policy Research

767 3rd Ave Floor 35, New York, NY 10017

This Working Paper is an output of the UNU-CPR initiative, "A Breakthrough for People and Planet: Building Momentum for the Summit of the Future and Beyond".

UNU CPR

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Global Challenges Foundation

unu.edu/cpr