Legal basis for processing biometric data from refugees

An analysis of the GDPR and following practices

Candidate: 105

Word count: 13351

JUS399 Master Thesis
Faculty of Law

UNIVERSITY OF BERGEN

12 December 2022

Table of Contents

1. Abstract

Protection of personal data is the most important legal standard when collecting and processing biometric data from individuals. Iris and fingerprint scans are commonly used as identification in humanitarian action. This in formation falls under special categories of personal data in accordance with Article 9(1) of the GDPR, and needs to be processed properly to ensure the right to the protection of personal data and minimize risks.

The problem discussed in this thesis is related to processing of biometric data from refugees done by NGOs working in humanitarian action, specifically the processing of data from iris scanning technology. The usage of biometric data is becoming more common, and raises several questions in relation to how it can be processed for use in humanitarian action.

2. Abbreviations

CJEU – Court of Justice of the European Union

CTP – Cash Transfer Programme

ECHR – European Convention of Human Rights

EDPB – European Data Protection Board

EEA – European Economic Area

EU – European Union

GDPR – General Data Protection Regulation

ICRC – International Committee of the Red Cross

IDP – Internally displaced people

INGO – International humanitarian organizations

IO – International Organisation

NGO – Non-governmental Organisation

NRC – Norwegian refugee council

TFEU – Treaty on the Functioning of the European Union

UDHR – Universal Declaration of Human Rights

UN – The United Nations

UNHCR – The United Nations High Commissioner for Refugees

WFP – World Food Programme

WP29 – The Article 29 Working Party

3. Introduction

The right to private life and the right to the protection of personal data are closely related. Both strive to protect the autonomy of individuals by granting them a personal sphere in which they can develop freely. These rights are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression.

In recent years the interest in data protection has seen a rise from the general public and organizations all across the globe. It's hard to say if it is the increase in automated systems or an increased awareness that's responsible, but there are now more restrictions and rules around the processing of personal data than before.[1]

The introduction of the GDPR in 2018 has been an important step in strengthening these rights within the EU/EEA.[2] The introduction of the GDPR also affected how organizations working within these countries can operate. Organizations had to change their terms and conditions, and change their practices to ensure compliance.[3]

Humanitarian organizations often work with refugees[4] and internally displaced persons (IDPs)[5] who are in very vulnerable positions when it comes to their right to personal data, but the collection and processing of personal data from refugees is valuable both during aid projects and during the asylum process.

Humanitarian organisations often operate in situations where there may be a limited access to justice and respect of the international human rights framework. The refugees' right to control personal data is often abandoned to a certain degree in the face of more pressing issues concerning health and life. This makes it even more important to have solid protection laws for the processing of personal data.[6]

Personal data is collected and processed by humanitarian organizations in order to efficiently perform humanitarian activities. Examples are fingerprints or iris scans, biometric identifiers that are unique to the individual. According to Andrew Hopkins, chief of identity management and registration at UNHCR, biometric data is highly efficient and is being used to register people at refugees camps and monitor accounts so that there is not an overspend on distributing aid.[7]

The need for processing of personal data means that without equal access to mechanisms that enforce data protection laws, refugees are especially vulnerable to violations. In some cases, the misuse of personal data may have life and death consequences. As an example, disclosing a list of

1 The preceding directive to the GDPR was Directive 95/46/EC, known as the data protection directive. Data protection is not a new notion, but after the introduction of the GDPR, the regulations concerning data protection are stricter.
2 The GDPR is currently regarded as the toughest privacy and security law in the world according to GDPR.eu. '*What Is GDPR, the EU's New Data Protection Law?*'
3 The New Humanitarian, '*Aid agencies rethink personal data as new EU rules loom*'
4 Defined by the UNHCR as "people incapable or unwilling to return to their country of origin owning to a well-founded fear of being persecuted for reasons of race, nationality, membership in a particular social group or political opinion.", UNHCR, '*What is a refugee*'
5 Persons who have had to flee their home within the country where they live.
6 International committee of the red cross, *Handbook on data protection,* p. 28
7 Ensor, '*Biometrics in Aid and Development: Game-Changer or Trouble-Maker?*'

names of asylum seekers may endanger their lives,[8] because many law enforcement agencies are specifically tasked with finding, detaining or deporting them.

As an example, the UNHCR improperly collected and shared personal data from Rohingya refugees from Myanmar with Bangladesh. Bangladesh further shared this data with the Myanmar government[9] to verify people for possible repatriation.[10]

Although the GDPR sets forth rules for processing in the countries governed by EU and EEA law, its implementation in humanitarian aid present several challenges. This is especially the case when it comes to legal grounds for processing personal data, particularly when consent cannot be valid. Failure to comply with the guidelines trigger risks for the data subject in a vulnerable position, and can also hurt the reputation of the organisation in charge of the personal data in question.

3.1 Purpose

This thesis will focus on the systematic registration of refugees' personal data conducted by European NGOs[11] in refugee camps around the world, specifically the use of biometric data. There are several challenges when finding the correct legal basis for processing this kind of data from refugees. It is therefore important to analyse the possibilities to avoid a situation where already vulnerable people are further compromised.

The aim of this thesis is to provide an insight to the implementation of the GDPR in humanitarian action, and to explore what limitations GDPR places on the processing of biometric data done by NGOs in humanitarian aid situations.

To do this the legal framework provided by the GDPR must be analysed to see in what degree processing is covered, and what limitations are put on the processing of biometric data.

3.2 Methodology

The GDPR is the main source. This is currently the most extensive legal framework on data protection, and applies to all EU/EEA countries and operators conducting business in these countries.[12] The GDPR is supplemented by recitals that are provided to further explain the contents of the articles. Recitals are used by the CJEU when interpreting the GDPR, and they are a valuable source to understand the nuances of the legal text.

The WP29[13] and the EDPB[14] also give guidelines, recommendations and best practices in relation to the GDPR. This guidance promotes a common understanding of the GDPR across the EU, and provides practical guidance and interpretative assistance in relation to specific articles under the GDPR. The opinions published by the WP29 are from before the GDPR came into effect in 2018, but they provided a lot of the background for the creation of the GDPR. The WP29 documents are

8 Human Rights Watch, '*UN Shared Rohingya Data Without Informed Consent*'
9 Human Rights Watch, '*UN Shared Rohingya Data Without Informed Consent*'
10 The return of someone to their own country.
11 An NGO is a non-profit organization that operates independently of any government. Typically NGOs will have a purpose related to addressing a social or political issue.
12 GDPR article 2(2)
13 WP29 was the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018.
14 The EDPB replaced WP29 after May 2018.

therefore still relevant for understanding the GDPR. Guidelines from the EDPB are published after the implementation of the GDPR, and provide clarifications that has been deemed necessary.

A deeper understanding of the general principles can also be gained from case law from the ECHR and CJEU. In many cases the case law is connected to cases from before the GDPR, but they are part of the basis that formed the legal framework for the regulation. They provide insight to the understanding of the specific articles. Case law from EU countries can also be relevant, as they have to adhere to the GDPR in national cases.

The existing literature on the GDPRs application in humanitarian action and NGOs is relatively limited, but some articles on the processing of biometric data including finger prints and iris scans have been written.[15] These articles provide a valuable insight into how personal information from refugees has been used by NGOs in the past, and how its currently being used today. The legal reach of the GDPR when it comes to cross border application has also been discussed by Christopher Kuner.[16]

Based on the information from articles and humanitarian reports, the goal is to simulate a hypothetical, but realistic, scenario of how biometric data is used by an NGO working with refugees. With a specific scenario in mind we can analyse the legality of processing in light of the GDPR, to see how the regulation provides limits to how biometric data can be collected and used.

Handbooks on data protection from the ICRC and WFP are also used to exemplify certain scenarios, as these organisations work with humanitarian aid on a big scale.

3.3 Delimitations

Humanitarian sector involves a large number of actors, such as IOs and NGOs as well as national and local authorities and private entities. The thesis will only focus on the work done by NGOs (an under-group of humanitarian organisations) that provide direct humanitarian aid to people in need during humanitarian action. This means that any processing done by the government or in relation to granting asylum will not be analysed. Many of the central problems and arguments will however also be relevant in regards to analysing a potential situation related to the asylum process within the EU.

The technical aspects of the collection, and data transfers to a third country will also not be discussed. This thesis will also not adopt a child perspective, and disregards the specific rights of children in relation to the processing of personal data.

This thesis will only look at the legal bases for processing that are relevant to the processing of biometric data, and will thus only be looking at article 9(a), (c), (d) and (g) in closer detail. This means that the other special categories of personal data, like health data and ethnic data in article (9) (2) or the legal grounds in article 6 will not be explored.

15 See for example UNHCR Innovation, '*Using Biometrics to Bring Assistance to Refugees in Jordan*', Rahman et.al. '*Biometrics in the Humanitarian Sector*' and The New Humanitarian, *'Eyes Wide Shut: The Challenge of Humanitarian Biometrics'*

16 Kuner, '*International Organizations and the EU General Data Protection Regulation*' and Kuner, '*The GDPR and International Organizations*'

3.4 Outline

Before discussing the main problem of legal basis for processing personal data from refugees, central terms and definitions used in the GDPR will have to be explained. Understanding the concept of "personal data" and "processing" is especially important. This will be addressed in chapter 4.1 and 4.2 respectively.

The legal reach of the GDPR also needs to be commented on, due to the fact that many NGOs work across borders and are international in nature. International organisations (IOs) benefit from certain immunities and privileges in the legal sphere,[17] and the legal reach will therefore be briefly commented on in chapter 4.3.

Because the GDPR is complex, and there are many situations that could provide challenging in relation to processing personal data from refugees, it is useful to look at a specific situation. In this thesis an example situation is created in chapter 5 based on earlier practices and current challenges NGOs face in light of humanitarian aid work. This example is only meant as an illustration, and is not intended to represent an actual situation or NGO currently providing humanitarian work. It is also not intended to directly criticize the way certain NGOs currently provide aid in similar situations.

With a specific situation at hand, the main part of this thesis will be focused on the legal basis for processing biometric data in accordance with the GDPR article 9. Generally the processing of personal data that falls under special categories of personal data is illegal according to GDPR article 9(1) unless one of the exceptions in article 9(2) apply. During humanitarian aid NGOs will often want to process data that falls under the special categories of personal data because of the way it excels at identifying individuals. It is therefore important to look into the exceptions in GDPR article 9(2) in detail, which will be done in chapter 6.

The legal basis in article 9(2) is however not the only important aspect to processing biometric data, and the guiding principles in GDPR article 5 must be discussed. This is done in chapter 6. Chapter 6 also contains information about security and further processing, two very important parts of processing in humanitarian action.

4. NGO practices and processing of personal data

4.1 Data collected during humanitarian aid

NGOs working in the humanitarian sector generally provide aid to people in need through distribution of food, clothing, medical services and cash in situations of humanitarian crisis, such as war and natural disasters. To ensure that the right people are receiving aid, NGOs typically collect information to identify these individuals. Organizations in the humanitarian sector routinely use new technologies such as data analytics, biometrics, cloud services and messaging apps[18] to make the process more effective. A concrete example is the UNHCRs usage of iris scan to withdraw cash for Syrian refugees in Jordan[19] in 2015.

17 See for example UN General Assembly, '*Privileges And Immunities of The United Nations'*, article 2 section 2
18 Kuner, '*International Organizations and the EU General Data Protection Regulation*' p. 4
19 '*The Individualisation of War | Eye Scan Therefore I Am: The Individualization of Humanitarian Aid'* and The New Humanitarian. '*Eye Spy: Biometric Aid System Trials in Jordan*'

A report by the UN published 10th of November 2020 notes that UNHCR requires refugees returning to camps in Afghanistan to undergo mandatory iris scan and registration to receive assistance.[20] This was justified as a preventive measure to detect and prevent fraud, but the implications of making such registration mandatory is severe because of the consequences a data breach could potentially have. The impact of such systems can be dire if it is flawed or abused, and the report indicates that the current practices put refugees at unnecessary risk.[21]

Acquiring biometrics from persons of darker skin colour or persons with disabilities can generally be more difficult, and fingerprinting can generally be difficult to undertake correctly if fingerprints are less pronounced due to manual labour.[22] Facial recognition also generally works worse on dark skinned individuals.[23] This can lead to some refugees not getting access to food or necessary aids for survival if too much trust is put in the system. If the system is abused, it could also lead to refugees being identified for other purposes than receiving aid.

Refugees are generally expected to give information about their name and residence, but also information about surviving sexual violence, torture, war crimes or crimes against humanity.[24] Requiring biometric data, like fingerprints, facial recognition and iris scan, has also become common among both UN agencies and NGOs.[25]

The personal data required varies depending on the concrete situation. The personal data required by aid organizations or governments also vary slightly between different EU-countries and NGOs, but generally the majority of data handled by aid actors are particularly sensitive in nature.

4.1.1 Personal data

NGOs collect what the GDPR defines as "personal data" from the refugees[26] in question. According to the GDPR article 4(1), personal data is defined as "any information relating to an identified or identifiable natural person(...)".[27] The GDPR regulates the collection, storage, and processing of this kind of data.

Usage of the term "any information" indicates that the regulation is meant to cover large amounts of information, regardless of nature, content or form. Practice from the CJEU supports that the term should be interpreted broadly.[28] This means that the concept of personal data includes any sort of information about a person.

Furthermore it is specified that the information must be connected to an identified or identifiable individual. An "identifiable […] person" is defined as "one who can be identified, directly or indirectly".[29] This means that the information must be connected to a specific individual, as opposed to a group of people. To determine whether a person is identifiable, the controller must take into

20 The New Humanitarian. '*Eye Spy'*
21 ComputerWeekly.com. '*Humanitarian Data Collection Practices Put Migrants at Risk*'.
22 Breckenridge, '*The Biometric State: The Promise and Peril of Digital Government in the New South Africa,'* p.275
23 Furl et.al. '*Face recognition algorithms and the other-race effect: computational mechanisms for a developmental contact hypothesis'*
24 Kaurin, '*Data Protection and Digital Agency for Refugees*'
25 Kaurin, '*Data Protection and Digital Agency for Refugees*', p.7
26 From here on regarded as synonymous with "data subject"
27 GDPR article 4(1)
28 See the cases Breyer, C-582/14 and, Nowak, C-434/16
29 GDPR article 4(1)

account all reasonable means that are likely to be used to directly or indirectly identify the individual.[30]

Direct identification refers to techniques that can identify a person directly, such as ID-numbers, where the information alone provides certain identification. Indirect identification refers to use of several identifying factors, such as the combination of name and address.[31] Indirect identification can also be done through phone numbers, IP addresses or photos with identifiable people.[32] It is important to note that the information does not have to be identified with a person to be covered by the definition, following the usage of the word "can". It is sufficient that the information in any way can be identified with a specific person in the future. Data that does not include identifiers are commonly regarded as anonymous and are outside the scope of GDPR.[33]

According to Recital 26, the benchmark for whether information is considered personal data or not is whether it is likely that reasonable means for identification will be available and administered by the foreseeable users of the information. It also follows from C-184/20 (Vyriausioji tarnybinės etikos komisija) that a person can have their data identified through a relation, even if their personal data was not part of what was originally collected.[34]

The regulation also only applies if the subject is a "natural person". This means that the GDPR does not apply in cases where the data subject is a juridical person such as corporations and firms, and does also not affect data connected to a deceased person.

Based on the definition in article 4(1) and the affiliated source material, most information about an individual must be considered "personal data". There must however be a lower limit for what constitutes as personal data, otherwise material scope of the GDPR would be too broad.

Generally, the identification of the data subject must be sufficiently precise. This is an overall assessment, where motivation for identification, access to required techniques, information, economic resources and expertise to complete the identification are aspects of the evaluation.[35] The cost, time, and available technology should also be taken into account.[36] Using several different datasets together can result in uncertain results, and this data must reach a certain level of certainty.[37] Certain types of personal data are however sensitive in nature, and will need stricter data protection rules.

4.1.2 Special categories of personal data

The GDPR has its own category for personal data that is sensitive in nature, known as "special categories of data"[38] in article 9. This kind of personal data need stricter guidelines to protect the individuals sufficiently.

30 GDPR recital 26
31 Schartum, *Personvernsforordningen – en lærebok*, p.44
32 Gruschka, et.al, '*Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*'
33 GDPR recital 26
34 Vyriausioji tarnybinės etikos komisija, C-184/20, paragraph 42
35 Schartum, *Personvernsforordningen,* p. 44
36 GDPR Recital 26(4)
37 Schartum, *Personvernsforordningen,* p.44
38 In Directive 95/46/EC, The predecessor of the GDPR, this category was known as "sensitive data".

What is regarded as special categories of personal data follow from the GDPR article 9(1), and includes personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "genetic data, biometric data, [...] data concerning health or data concerning a natural person's sex life or sexual orientation."

Generally the definition of special categories of data also seem to be very broad. This is again highlighted by C-184/20 (Vyriausioji tarnybinės etikos komisija), where the CJEU ruled that processing personal data liable to indirectly reveal sensitive information concerning an individual is also prohibited under the GDPR unless an article 9(2) condition applies.[39] This clearly highlights how broadly special categories of personal data are defined, and also how strict the legislation is. There are however 7 defined categories of what constitutes as "special categories of personal data".[40] This thesis focuses on the processing of "biometric data", and will therefore not go further into the definitions for the other special categories of personal data.

"Biometric data" is defined as personal data resulting from "specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".[41]

This indicates that any recognizable and unique feature on the body of a human is to be regarded as biometric data. Biometric data will therefore include biological properties, physiological characteristics, living traits or repeatable actions where those features are individually unique and measurable. Typical examples are fingerprints, retinal patterns, and facial structure, but also voices, hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristics such as handwritten signatures are included.[42]

Even if facial images are listed as an example in GDPR article 4(14), it should be noted that the processing of photographs is not considered to be processing of special categories of personal data. They are only covered by the definition if they are processed using techniques that allows for the unique identification of a natural person.[43] This is what we see in facial recognition tools, where the program analyses specific features to provide a unique identification.

Blood, spit and other tissue samples are in themselves not biometric data unless they have been processed to extract identifiable information. A pattern for fingerprints is biometric data, but the finger itself is not.[44]

Biometric data excels in differentiation one human from another. It is also based on permanent identifiers that cannot be changed in any way. Biometric data is thus a precise identification method, which is especially useful in situations concerning refugees. There is no way to trick the system to gain for example double rations by acquiring another persons identification card.

Biometric data is often collected by NGOs and other organizations to ease the identification process. The usage of fingerprints and iris scan in relation to food distribution has already been mentioned, and generally the trend is that biometric data is becoming more and more common.

39 Vyriausioji tarnybinės etikos komisija, C-184/20, paragraphs 120-128
40 GDPR article 9(1)
41 GDPR article 4(14)
42 Opinion 4/2007 on the concept of personal data, WP136 p.8
43 GDPR Recital 51
44 WP136 p.9

Fingerprints, face recognition and iris scans are for example turning into the norm for identification in technology from Apple.[45]

4.2 Processing of personal data

The personal data in question will have to be collected and used in some way, and in the context of the GDPR this is known as "processing". According to GDPR article 4(2) "processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data", including "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

This is again a very broad definition. The requirements for an operation to be defined as "processing" are seemingly very low, to the point that any operation done is covered. Processing can also consist of several operations on the same dataset, like collecting, analysing and structuring the personal data in question.[46]

The definition given in the GDPR does not provide guidelines on how to tell one form of processing from another, but it is natural to look at the purpose for the processing to differentiate different operations. The connection between purpose and processing has a long tradition in privacy law, even though purpose is not specifically defined in the GDPR. It follows from GDPR article 5(1)(b) that two operations towards the same purpose would generally be viewed as one "processing" because they are directly linked. An example would be collecting iris information and putting said information into a register.

4.3 Legal reach of the GDPR in relation to NGOs

The GDPR is an EU regulation, which means that it is binding for any EU member states.[47] In these countries, the regulation has immediate effect and direct application.[48] This means that the GDPR is independent of national law, and organisations have to adhere to the regulation directly.

The GDPR is also binding for the EEA states Lichtenstein, Iceland and Norway. In the case of Lichtenstein, EU regulations are direct law according to the national constitutional law. For Norway and Iceland, the regulation must be implemented in national law according to the EEA agreement article 7(a).[49]

The GDPR also has a territorial scope outside the EU/EEA nations, but it is not globally binding. This is especially relevant when discussing situations related to international organizations (IOs) because these organizations have certain immunities and privileges in relation to international and national law. An example of a privilege can be exceptions from the substantive law of a state, and immunities are exceptions from legal process or enforcement.[50]

45 Apple Support, *'About Face ID advanced technology'*
46 Schartum, *Personvernsforordningen,* p.49
47 TFEU 2016 article 288(2)
48 Variola, C-34/73
49 Kokott, C-431/11
50 Kuner, '*International Organizations and the EU General Data Protection Regulation*' p. 17

The GDPR defines an IO as an "organization and its subordinate bodies governed by public international law, or any body which is set up by, or on the basis of, an agreement between two or more countries".[51] This definition is also widely used by other sources.[52]

GDPR article 3(1) states that the GDPR "[…] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.".

The definition given in article 3(1) means that an organisation with a main office or department in the EU will qualify as having an EU establishment. Many NGOs are EU based. Examples include the Norwegian refugee council (NRC) based in Norway, and War Child Holland (WCH) from the Netherlands. Also more global organisations like the UN and ICRC have offices in the EU, and will therefore fulfil the requirements.

Immunity to certain legal procedures could however mean that NGOs could potentially be exempt from the GDPR. This is especially relevant for the bigger organizations like the UN and ICRC. The bigger organisations, that are almost unrivalled in their purpose, will therefore have broader immunities and privileges. These are important tools to ensure the organisations can fulfil their purposes and functions.

The GDPR does not address the issues regarding the general application in cases where there could be certain conditions standing in the way of full application, like cases of international legal immunities. CJEU has not yet issued a clear pronouncement on the status this with respect to EU law. Based on the fact that EU is required to respect the principles of the UN charter,[53] it can still be argued that the EU should respect the immunities and privileges given to widely recognized aid organisations like the UN, ICRC and WFP.

At the same time, these organisations have clearly expressed their intention to follow the GDPR as closely as possible. ICRC has created their own guidelines[54] that closely follow the GDPR, as a way of ensuring that data protection law is applied in all cases of humanitarian aid. It is also important to note that the privileges and immunities are granted by member states, which again means that they are not necessarily granted by an interstate organisation like EU.

A recent case by the CJEU, C-131/12 (Google Spain), also raised questions about the extent of the territorial scope of the GDPR. The CJEU held that the Directive applies to processing by Google to provide search results in Spain, despite the fact that Google Inc. is based in California. This was the case even if it is Google Inc. that provides search services in Spain.[55] This emphasises the fact that the GDPR applies in cases where international bodies have branches within Europe.

The discussion on this is complicated, and no definite answer has been given at present time. For the further purpose of this thesis, it will be assumed that the GDPR applies to all NGOs working

51 GDPR article 4(26)

52 "International organization" looked up in Practical Law. '*International Organisation*', Law Insider. *'International Organisations Definition*', National Geographic society, '*International Organization | National Geographic Society*' and OECD Glossary of Statistical Terms, '*International organisations Definition*'

53 TFEU 2016 Article 3(5)

54 ICRC *'Handbook on data protection'*

55 Google Spain and Google, C-131/12

intentionally with connection to the EU, according to the principle of territorial reach in the GDPR.[56]

The GDPR also has a material scope for what types of information it applies to. It follows from article 2(1) that the GDPR "[...] applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Because of the broad definition of "data processing", as discussed above in chapter 4.2, the regulation will apply to almost any operation that can be performed on personal data. The material scope will therefore rarely cause problems, as long as the data in question falls under the definition of "personal data".

5. Processing of biometric data in relation to CTP

To better understand the possible legal grounds available to an NGO doing humanitarian work, it would be appropriate to look at a concrete example and analyse the situation in light of the GDPR.

In February 2022, the Russian Federation launched an offensive against Ukraine that has resulted in millions of people being driven from their homes to search for safety. The country is still plagued by war in the time of writing this thesis, and many different organizations are currently performing aid projects in Ukraine. NGOs providing aid includes, but is not limited to, the NRC (Norwegian Refugee Council), DRC (Danish Refugee Council) and project HOPE (health opportunities for people everywhere).

A tool that is often used in humanitarian emergencies is Cash Transfer Programming (CTP), where refugees are provided with cash to help them survive day to day life. Using CTP maximises the respect for beneficiaries' choices.

Major humanitarian crises such as the Asia Tsunami (2004), Pakistan earthquake (2005), Haiti earthquake (2010), Pakistan floods (2010), Horn of Africa and Sahel (2011), Syrian refugees (2012) and more recently Philippines (2013), have all used CTP as aid.[57] CTP is also currently being used in Ukraine by the NRC.[58]

For CTP to function, the NGO in question needs to process individuals' personal data to identify the people in need of aid, and ensure that the correct individual receives said aid. Personal data collected during this process typically includes full name, mobile phone number, geolocation/other phone metadata and biometrics.[59]

When UNHCR began its cash assistance program in 2008 the refugees initially received bankcards and PIN numbers to make their withdrawals. But cards were lost or PINs forgotten, and sometimes refugees would give their card to another family when they moved. To overcome these difficulties, UNHCR decided to employ biometrics for the cash assistance project.[60]

56 GDPR article 3(1)
57 EU, '*10 common principles for multi-purpose cash-based assistance to respond to humanitarian needs*'
58 Norwegian refugee council, '*First Distribution of Cash to Ukrainian Refugees | NRC*'
59 ICRC *'Handbook on data protection'* p.149
60 UNHCR Innovation, '*Using Biometrics to Bring Assistance to Refugees in Jordan*'

For our example, we will assume that an NGO[61] working in Ukraine wants to use iris scan[62] as the main identifier to ensure fast, fair and efficient distribution of cash aid to refugees.[63] Using iris scan is justified with reference to the chaotic situation, and the high likelihood of physical documents like ID papers getting lost, stolen or counterfeit.

The NGO is also very interested in using new technologies, and iris scan is seen as a better way of identification than fingerprints. Iris scans are known to be superior at identifying individuals correctly. Even genetically similar people have entirely independent irises. Iris scanning recognition can even avoids misidentification of identical twins.[64]

This fictive situation is very similar to how iris scans have been used in humanitarian action over the years in relation to food distribution[65] or cash aid.[66]

5.1 Material and territorial scope of the example

Data gathered from iris scan will fall under the definition of "biometric data" in GDPR article 9, see chapter 4.1.2. It is also clear that the collection and systematization of information gathered from an iris scan falls under the definition of "processing". An operation is carried out, and the information can identify a specific individual. The collection and usage of iris information will therefore fall under the material scope of the GDPR, see chapter 4.3.

Ukraine have status as an EU candidate as of 23. June 2022, but is currently not a part of the EU. The territorial reach of the GDPR will therefore not apply unless the NGO in question is located in an EU country.

We will in the following assume that the NGO in question is located in an EU country, so the territorial reach of the GDPR pose no problem. We have already established in chapter 4.3. that organizations working outside the EU is still bound by the GDPR as long as they have office in an EU country. The NGO is therefore bound by the GDPR.

6. Legal bases for processing biometric data in relation to CTP

The use of biometric technologies like iris scans raises significant data protection issues. An iris scan may potentially enable the extraction of sensitive information beyond the identification of the individual. Iris information can also be read from a distance, thus making it particularly sensitive.[67] It is therefore particularly important to ensure that any processing of this information is done in compliance with the GDPR.

---

61 The "controller"

62 According to ID, IRIS, '*What Is the Difference between Iris Recognition and Retinal Scanning?*', iris scans are superficial registration method involving taking photos of the iris, the coloured ring around the pupil. Another way of doing eye scans are retinal scans, which require a more intrusive process to get a photo of the retina sitting at the back of the eye. Iris scans are much more common because of the non-intrusive method.

63 The "data subject"

64 Lu et.al. 'A *Study of Personal Recognition Method Based on EMG Signal*" and Tao et.al. '*Fingerprint Recognition with Identical Twin Fingerprints*'.

65 The New Humanitarian, '*Eye Spy: Biometric Aid System Trials in Jordan*'

66 The New Humanitarian, '*Eye Scan Therefore I Am*'.

67 ICRC '*Handbook on data protection'* p.131

GDPR article 9(1) prohibits any processing of personal data that falls in under the special categories of personal data, but there are several exceptions in article 9(2) (a)-(j) that allows for processing in specific scenarios. This list is exhaustive, and should not be interpreted expansive.[68]

The most relevant of the exceptions given in article 9(2) in relation to processing special categories of personal data from refugees in humanitarian action are article 9 (2)(a) – consent, (c) – protection of vital interests, (d) – processing carried out in the course of legitimate activities and (g) – reasons of substantial interest.

Consent is the most popular and often the preferred legal basis for processing of personal data, but given the vulnerability of refugees receiving aid and the nature of humanitarian emergencies, it can often be impossible to rely on consent for processing of personal data in these cases.[69]

It might be more appropriate for an NGO to look at for example vital interests and legitimate interest before considering consent, but it is important to understand why consent can be problematic in these situations. In cases where consent can be valid, it is however the most preferable legal basis according to the ICRC. Humanitarian organizations should only use alternatives in cases where it's impossible or impractical to obtain valid consent.[70] In the following we will therefore first look at consent as a legal basis, before looking at the other possibilities.

6.1 Explicit consent following 9(2)(a)

According to article 9(2)(a), processing of special categories of data is legal in any case where the data subject has given "explicit consent" to the processing of those personal data for "one or more specified purposes".

According to article 4(11) “consent” means any "freely given, specific, informed and unambiguous indication" of the data subject's wishes given through a "clear affirmative action" that signifies "agreement to the processing of personal data relating to him or her". The conditions for consent are cumulative, which means that the threshold for consent to be legal is high. This supports the generally strict interpretation of the GDPR.[71]

6.1.1 Freely given

The condition that consent must be "freely given" is intuitively understood as a requirement for the consent to be given under conditions where the data subject is not pressured in any way to provide the consent. According to the "Guidelines on consent under regulation 2016/679", the element of "free" implies that the subject must have a real choice.[72] As a general rule, if the subject feels compelled to provide the consent or will suffer negative consequences if they don't consent, the consent will not be valid.[73] This means that any inappropriate pressure or influence on the data subject will render the consent invalid.[74]

68 Kuner et.al, *The General Data Protection Regulation: a commentary*, p. 375
69 ICRC, '*Handbook on data protection'* p. 61
70 ICRC, '*Handbook on data protection'* p. 151-152
71 Kuner et.al, *The General Data Protection Regulation: a commentary*, p.181
72 Guidelines 05/20 on consent under Regulation 2016/679 article 13
73 Opinion 15/2011 on the definition of consent, WP187 p.12 and GDPR recital 42
74 GDPR recital 14

As an example, there was a case in 2020 where an elementary school collected fingerprints from students in Poland. The fingerprints were used to identify the children in the school canteen, and the children who refused to have their fingerprints collected were put last in line. This meant that the children had clear negative consequences of refusing. The UODO[75] ruled that this was a clear breach of consent, both because of the negative consequences and also the fact that the students were dependent on the school.[76]

This case also highlights the fact that any clear imbalance between the data subject and the controller will pose a problem even if there is no direct pressure. It follows from recital 43 that consent should not provide a valid legal ground in these cases. WP189 uses an employment relationship as an example of such a power imbalance.[77] The guidelines on consent pull out the same example in article 21 and 22.[78] In an employment relationship the data subject is under the influence of the data controller, and the data subject could in this case be dependent on the data controller because of the nature of their relationship. The worker is in theory able to refuse, but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and therefore not valid.[79]

Another example can be seen in C-291/12 (Schwarz)[80] where the question was if the requirement of taking fingerprints in relation to issuing passports were legal. The CJEU noted that passports are essential to the citizen, and consent can therefore not be considered freely given.[81]

In regards the humanitarian sector, it is clear that refugees are in a position of dependence with respect to the aid organisations. The power imbalance in humanitarian aid is also generally very big, as it is often the data subjects lives that are at stake. It is very clear that the data subjects are dependent on the aid they receive. This makes consent hard to use as a valid form of processing special categories of data, as it will never be truly freely given.

In our example, the NGO requires the access to biometric data to provide cash aid. In the case of no real alternative methods of accessing the aid, this is not real choice. The refugees are often dependent on the aid they receive. In the case of not consenting to the processing, the refugees in question will lose the option to receive aid from the CTP. This is a clear negative consequence.

Reports from interviews done by Oxfam suggest that UNHCR has adopted the approach that refusal to submit to biometric registration amounts to refusal to submit to registration at all.[82] This also seems to be the understanding from the refugees themselves.[83] The refugees generally see registration of their biometric data as something they cannot refuse.

To get around this, the NGO could provide an option to use other means of identification to the ones refusing iris scan. It is however important that the refugees are clearly informed about this option. If the information is not readily available and actively given, there it still no semblance of a choice.

75 Urząd Ochrony Danych Osobowych, the Polish personal data protection office
76 *'Fine for processing students' fingerprints imposed on a school | European Data Protection Board'*
77 WP187 p.13
78 EDPB Guidelines 05/20 on consent under Regulation 2016/679, EDPB 05/2020
79 Opinion 8/2001 on the processing of personal data in the employment context (WP48) page 23
80 Schwartz, C-291/12
81 Schwartz, C-291/12, paragraph 32
82 Rahman et al. '*Biometrics in the humanitarian sector'* p.11
83 The New Humanitarian, '*Eye Spy*'

It is also important to note that the consent can be valid even if there is a clear negative consequence of not consenting if the consent is given in connection to a service requested by the data subject. If the service is dependent on the processing of personal data to be fulfilled, it can be valid according to article 7(4). An example situation can be postal delivery, where the consent to process name and address is a requirement for package delivery.

This is however not the case here, as identification can be done through other means. In the case from Poland mentioned above this was one of the key arguments as to why the processing was illegal. Already we can see that consent is not an ideal legal basis for processing in our example, unless the NGO offers alternative methods to receive aid. If the NGO does provide an alternative form of access, consent can however still be valid if the remaining requirements are fulfilled.

6.1.2 Specific

Next, the consent must be "specific". A natural understanding of "specific" is that the consent needs to be directed towards a concrete situation at hand, and given in relation to the action of collecting the personal data required in this situation. It follows directly from GDPR article 9(2)(a) that the consent needs to be specific towards the processing actions the controller wants to perform. If the purpose is "vague or general", consent cannot be valid.[84]

The purposes for the data processing must in other words be clear, and the consent must be tied to a specific data set or categories of data that the controller will be allowed to process for the stated purposes. This ties into the requirements in article 5(1)(b) that calls for the determination of a specific, explicit and legitimate purpose of the processing. This means that the consent is tied only to the processing that is defined in the initial information given. No processing outside this purpose is allowed.

In our case this does not pose a big problem, as long as the NGO clearly states the purpose when they ask for consent to processing of biometric data.

6.1.3 Informed

Closely related to the requirement for specificity, is the fact that the consent must be "informed". A general understanding of this requirement is that the data subject must know what they are consenting to. This is in line with the principle of transparency in GDPR article 5. Providing information prior to obtaining consent is essential in order to enable data subjects to make an informed decisions on whether to consent or not. If the controller does not provide sufficient information, consent will be invalid.[85]

The data subjects must in other words fully understand what they are agreeing to. The controller should generally ensure that they use clear and plain language so the data subject can easily understand the situation.[86] According to EDPB, the information must also include what kind of data is being processed, the possibility of withdrawing consent[87] and any possible risks connected to the processing.[88]

84 Opinion 4/2007 on purpose limitation, WP203 p.16
85 EDPB 05/2020, paragraph 62
86 EDPB 05/2020, paragraph 67
87 In accordance to GDPR article 13(2)(c) and article 14(2)(d)
88 EDPB 05/2020 paragraph 64

In C-673/17 (Planet49), the company Planet49 arranged an online competition where the winners would get a Macbook. To participate, the contestant had to fill inn personal data and make a decision related to two checkboxes. One of the checkboxes asked to place additional cookies on the contestants browser, to personalise advertisements. The problem was that the checkbox was pre-filled, and it did not contain enough information. The court ruled that it was a definite requirement to provide sufficient information to the users about storage time of the cookies and the fact that third parties could access this information.[89]

It is also a requirement that is must be clear that the data subjects have received said information according to C-61/19 (Orange Romania).[90] It is also the controllers responsibility to demonstrate that the subject has received the information, and to ensure that the information is given in a clear and understandable way.[91]

Providing sufficient information in relation to processing of biometric data can be challenging because of the sheer amount and the complexity of information required to fully inform about the risks and benefits of processing. The NGO would have to provide information[92] in the native language, provide the option of using other identification methods in case of refusal, and ensure that the subjects are able to withdraw consent at any time. In case of withdrawal data needs to be deleted in accordance with GDPR article 17.

In our example we are looking at relatively new technology that can be difficult to understand. It is therefore likely that it is difficult to provide sufficient information, and ensure that all of the data subjects have an adequate understanding. This is supported by the fact that refugees in general have little understanding of how their biometric data is used.[93] Ukraine is generally technologically developed, but iris scan technology is still very new. Even when provided with information about how the scan works, it is highly unlikely that the refugees will fully the technology and the implication of what the data could actually be used for if it should somehow get leaked or extracted by malicious third parties. The requirement for consent to be informed is therefore problematic.

6.1.4 Unambiguous indication

Valid consent also requires an "unambiguous indication"[94] from the data subject. This indicates a clear affirmative action that cannot be misunderstood or misinterpreted. The requirement of an "indication" of the data subject's wishes clearly points to an active indication, rather than a passive one. This understanding is supported by the "Guidelines on consent". The guidelines state that the consent must be given through an "active motion or declaration that clearly indicates the wish to consent to the particular processing".[95] The data subject must have taken a deliberate action to consent.[96] This means that passive behaviour cannot be viewed as consent.

89 Planet49, C-673/17
90 Orange Romania, C-61/19, especially paragraph 37
91 C-61/19 (Orange Romania), paragraph 40
92 In accordance with GDPR article 13
93 The New Humanitarian. '*Eyes Wide Shut: The Challenge of Humanitarian Biometrics*' and Kaurin, '*Data Protection and Digital Agency for Refugees*', p.11
94 GDPR article 4(11)
95 EDPB 05/2020, paragraph 75
96 EDPB 05/2020, paragraph 77

Planet49 also underlines this requirement. The court points out that "[consent] is not validly constituted if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect to refuse his or her consent."[97] This goes directly against the principle of an unambiguous indication, which requires an active action. Consent given in the form of a preselected tick in a checkbox does not imply active behaviour.

Iris information may only be collected directly from the data subject. The data subject must be present, and the action of collection must be performed directly on them. It should therefore be feasible and practical to obtain consent through an "unambiguous indication" by making the data subject sign or agree before collection.

6.1.5 Explicit

When processing special categories of data there is one additional requirement for consent to be valid. The exception in article 9(a) is based on the data subjects "explicit" consent. The threshold for "explicit consent" is understood to be higher than "consent". It must satisfy all the conditions given under the definition given in article 4(11), but the sensitive nature of the data involved requires a consent that goes beyond the regular "statement or clear affirmative action".[98]

It follows from the guidelines on consent that the term "explicit" means that the data subject must give "an express statement of consent".[99] The term "explicit" also means that the consent cannot be implied,[100] and requires a high degree of precision.[101] An obvious way to do this would be to give a written statement. This removes doubt and ensures future evidence.[102]

A signed written statement is not as practical in the digital or online environment, so other means will need to be used instead. The guidelines of consent recommends e-signatures, two step verification or electronic forms in this case.[103] Recital 95 also states that explicit consent can be obtained through a telephone conversation, if the information about the choice is "fair, intelligible and clear" and it asks for a "specific confirmation" from the data subject. Examples of this would be pressing a button or providing an oral confirmation.[104]

In theory, the use of oral statements can also be sufficient to obtain valid explicit consent. It may however be difficult to prove that all conditions for valid "explicit consent" were met when the statement was recorded.[105]

Generally this should also not pose a problem in our example, as the refugees need to be present for the iris scan to be performed. It is feasible for the NGO to provide a way of consenting to the scan and processing through a written statement.

97 Planet49, C-673/17, paragraph 63
98 GDPR article 4(11)
99 EDPB 05/2020, paragraph 93
100 When consent is implied, it is generally inferred from signs, actions, or facts, or by inaction or silence.
101 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.377
102 WP187 p. 25
103 EDPB 05/2020, paragraphs 94 and 98
104 WP187 p. 25
105 EDPB 05/2020, paragraph 94

6.2 Vital interests

When consent cannot be validly obtained, biometric data can still be processed if any of the other legal bases apply. According to GDPR article 9(2)(c) processing special categories of personal data is allowed when processing is necessary to protect "the vital interests of the data subject or of another natural person" where the data subject is "physically or legally incapable of giving consent."

The scope of this exception is limited. It only applies to cases that concern the "vital interests" of the data subject. This indicates that the processing must be related to the health and safety of individuals. It follows from GDPR recital 46 that "vital interests" are interests that are essential for the data subjects life.[106] This includes safeguarding against threats to the physical integrity or life[107] of a person or a third person. In other words, it must be a matter of life and death. It may also apply to humanitarian situations such as providing relief for natural or man-made disasters.[108]

In difficult conditions like war, vital interests might constitute a plausible alternative legal basis for processing biometric data when the NGO is incapable of acquiring valid consent. Biometric data is especially effective at identifying individuals, and it can be argued that the usage of such biometric systems is in the data subjects best interests when the NGO has limited resources to provide aid by other means. In cases where the NGO is providing essential aid like food, water and medical assistance, this would be a legitimate reason, as the NGO is providing services that are required for the data subjects survival.

In our example, the NGO is using biometric data to provide cash aid that the refugees will use on what they themselves regard as important. It can seem hard to argue that cash aid is protecting vital interests, especially considering the high threshold. To be eligible to receive cash aid, the subject is not in a life threatening situation. On the other hand, cash aid is provided to people in need, and reports from the CTP done by NCR in Ukraine show that the refugees receiving cash aid spend the money mostly on food.[109] Food is an essential to live, and the cash could by extension be viewed as essential aid

The usage of a biometric system is however not essential to provide aid, and the usage of such systems seem closer related to the NGOs wish to carry out their work in an effective way. There are different ways of providing aid, and the use of biometric systems as identification is not the only option available. It is possible to for example use identification cards based on name, which would be a less intrusive way of providing aid based on identification. The usage of iris scan in this case is therefore closer related to the NGOs needs rather than the data subjects vital interests, and the CTP cannot be regarded a protecting vital interests even if it is providing the refugees with access to essentials like food and clothing.

Even if the usage of biometric data was in this case regarded as providing aid protecting the subjects "vital interest", the second condition in Article 9(2)(c) must be fulfilled. The data subject must be "incapable of giving consent" for the exception to be relevant. This drastically limits the application, as it can only be invoked when the subject either physically or legally cannot provide

106 GDPR recital 46
107 GDPR recital 112
108 GDPR recital 46
109 NRC, '*First Distribution of Cash to Ukrainian Refugees | NRC*'.

sufficient consent for processing. Examples can be if a person is unconscious or if they are incapable of consenting due to legal status, like being a minor. This also applies in cases where the subject is under duress and incapable of understanding the consequences of the decision.[110] The reason for this is the nature of special categories of personal data. Because this kind of data needs stricter protection, it is also important to ensure that actors cannot rely on the vital interests exception as an alternative option if a person is able to consent and has refused to do so. As a general rule, explicit consent should be requested whenever possible.

In the case of using iris scan to distribute aid, the exception of vital interests cannot provide sufficient legal grounds. The collection in this case is done when the data subject is conscious and awake, and it is highly unlikely that it is carried out in a situation where the data subject can be said to be under significant duress that makes them unable to consent.

Following this, the vital interest exception is mostly useful in medical emergency situations. An example can be where the data subject has suffered a life-threatening injury, and medical staff will have to check the medical history to decide the proper treatment. If a person is unconscious they will not be able to consent, and it is in their best interest to have the data processed to survive. Another example can be in cases of epidemics, where it may be impossible to get all infected individuals to consent in a timely manner. Medical staff will in this case need to process information as quickly as possible, to prevent further spread of disease. This is necessary to protect a third party's vital interests.

6.3 Legitimate interest of the NGO

The fact that the iris scan is in the NGO s interest could also provide a legal basis for processing. The exception in article 9(2)(d) makes it legal for "a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim" to process such data where it is "carried out in the course of [the organizations] legitimate activities".

The list of organizations covered by this exemption seem to be limited to the exact types listed, but this cannot be the case. The list must be illustrative because the legal status of charity and non-profit organizations is not uniform in the EU. The exact nature of the organization will depend on the legal form and structure member states give them.

The list of aims and goals of the organization in question will therefore be much more relevant to analyse. The organisation in question must pursue one of the aims mentioned. The aims listed refer to a limited number of activities, and cannot extend beyond this. The organization must also process the data in question only in course of their "legitimate activities", which means that it must be directly connected to the purpose of the organization. The exception also only applies to processing data from "members or people with regular contact with" the organisation.

Article 9(2)(d) covers non-profit organisations like political parties, youth groups, non-profit foundations and similar groups.[111] Non-profit organizations like NGOs are covered, but only in the cases where they have a purpose that aims to permit "the exercise of fundamental freedoms" to fall under this exception.[112] The organization must be organized on a non-profit basis, and must be

110 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.377
111 GDPR recital 51
112 Kuner et.al., *The General Data Protection Regulation: a commentary,* p.378

processed in relation to the core of the purpose of the organization. The processing must also be done exclusively internally in the organization, as the exception in GDPR article 9(2)(d) does not allow for processing that includes data transfer to third parties. Any disclosure of data requires the consent of the data subject.[113]

In our example, we are dealing with a non-profit organisation with the aim of aiding refugees through difficult situations. It is clear that the refugees are in regular contact with the NGO if they are to receive aid. Providing access to cash through a CTP will also be directly connected to the purpose of aiding refugees, as it will help them survive on a day to day basis. A legitimate interest for an NGO with this as its main goal, can be to process personal data that will make the delivery of aid more efficient and thus reach more people in need. Cutting down on paperwork by connecting recipients directly to the allowances they receive through an iris scan can be regarded as a more secure method of delivery. It ensures that the allowances are only used by the people they're intended for.[114]

It is however important that the legitimate interest of an organisation does not interfere with the fundamental rights and freedoms of the data subject, as biometric data like an iris scans can be used for potentially intrusive purposes. This means that it can be discussed if the rights of the data subject will always override an NGOs legitimate interest.

This does not have a definite answer, and it follows from C-582/14 (Breyer) that legitimate interest must be analysed on a case-to-case basis. This is a balancing between the controllers interests and the data subjects interests, rights and freedoms.

Important aspects could be the severity of the situation, the need to provide aid quickly and efficiently, the vulnerability of the data subject and the possibility of using other, less intrusive means of identification. The concept of reasonable expectations of the data subject will play a role. According to this criterion, the controller would need to assess whether the data subject reasonably expects the collection of the personal data at the time and the context of the collection for the specific purpose.[115] Another important aspect of this analysis is the necessity of the processing. This will be further commented on in chapter 7.2.

6.4 Reasons of substantial public interest

Lastly, biometric data can be processed in cases where it is "necessary" for "reasons of substantial public interest".[116] It is natural to understand this as something more than "public interest" which would be related to what is in the best interests of the society. "Substantial public interest" must go beyond this, and will be related to the exercise of fundamental rights and freedoms, like organizing the electoral process, or the maintenance of order and security and fighting terrorism. It follows from recital 46 that reasons of "important grounds of public interest" can include the vital interests of the data subject when processing is necessary for humanitarian purposes, for example in relation to epidemics or in situations of natural and man-made disasters.[117] The interest needs to be real and

113 GDPR Article 9(2)(a)
114 The New Humanitarian, '*Eye Spy*'
115 GDPR recital 47
116 GDPR article 9(2)(g)
117 GDPR recital 46

of a certain level of substance. The NGO must therefore be able to make specific arguments about the concrete benefits for the general public to reach the threshold laid down by the GDPR.

In our case we have already discussed the fact that using biometrics is more related to the NGOs interest than the data subjects "vital interest" following article 9(2)(c), but it is a right of a refugee to receive aid in humanitarian situations. It can therefore be argued that providing aid through a CTP benefits the general public by ensuring the refugees have resources to live on.

It is important to note that the exception in article 9(2)(g) is only triggered in cases where the activity in the public interest is laid down by "Union or Member State law".[118] This means that it is only relevant in those cases where NGOs are performing a specific task or function in the public interest and which is laid down by law, and the processing of personal data is "necessary" to accomplish those tasks. This will for example be the case when the activity in question is part of a humanitarian mandate established in national or international law. Similarly to the last exception of legitimate interest of the NGO, it is important that the processing of the specific personal data is truly "necessary" for the activity in question to be carried out.

7. Other important data protection principles – Article 5

In addition to being legal in accordance to article 9, the processing of biometric data must follow the other key principles laid down in GDPR to be legal. Article 5 of the GDPR summarize these principles, and these principles needs to be incorporated prior to data collection.[119]

Firstly, all personal data must be "lawfully" processed.[120] The principle of lawful processing must be understood in relation to conditions for lawful limitations to the right to respect private life in CFR article 52(1) and ECHR article 8(2).[121] Following this, processing of personal data should pursue a legitimate purpose, be necessary and proportionate in a demographic society to be considered lawful. The broad takeaway is that processing of personal data is only lawful if at least one of the conditions listed in article 6(1) or article 9(2) apply to the specific case. We have already discussed the lawfulness in relation to the conditions laid down in article 9 in chapter 6.1.

Emphasis is also put on the fairness and transparency of the processing. At the time of data collection, the data subjects must not be mislead, and they should always be made aware of the identity of the actor collecting their personal data as well as the purpose for collection. The GDPR emphasises that this information must be provided in a clear and plain language, preferably in the data subjects native language. This can lead to difficulties when it comes to people who originally reside outside the EU.[122] In our case this is especially tied into the concept of consent following article 9(2)(a), see chapter 6.1.

The principles of purpose limitation, data minimization and proportionality, and security are particularly important in a refugee situation and will in the following be further elaborated on.

118 GDPR article 9(2)(g)
119 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.311
120 GDPR article 5(1)(a)
121 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.314
122 Gazi, '*Data to the Rescue: How Humanitarian Aid NGOs Should Collect Information Based on the GDPR*'.

7.1 Purpose limitation

The concept of purpose limitation means that there must be a clear purpose for the processing from the start, and this purpose needs to be recorded and followed. What is considered as a legitimate purpose depends on the circumstances, but the purposes must be explicit and legitimate, and clearly communicated to the data subjects. An example of the importance is in regards to the definition of processing operations in chapter 4.2, and informed consent in chapter 6.1.3.

If the purpose changes over time, or the processor wants to use the data for a new purpose, there are limitations to whether this can be done or not. Using the data that has been collected for other purposes is only legal if it is compatible, there is consent from the data subject, or there is a clear obligation or function for the further processing set out in law.[124] The notion of compatibility has raised several questions in practice.[125] This will be further commented on in chapter 7.4, but generally the purpose determines which types of personal data can be processed, and to what degree this data can be processed.

In the case of CTP, the purpose should involve the provision of assistance to enable the target group to access the goods and services they need. The purpose should be clearly communicated to the individual or group of people in question no matter what the legal basis for processing turns out to be.

7.2 Data minimization and proportionality

The information collected must also be proportionate to the purposes. This is known as the concept of data minimization.[126] In short terms, this means that the actors should only process personal data that is adequate, relevant and limited to what is necessary[127] for the service they want to provide. Any excess information that is not relevant for identification purposes should not be collected. Consequently, it is necessary to establish whether refugees' biometric data processing is proportional to the need for identifying an individual in relation to CTP.

The distribution of food in a refugee camp would for example require the subjects full name and documentation to verify their residential status. Processing of other personal data such as martial status is not needed for conducting the distribution of food, and is therefore by the principle of data minimization not allowed. If there is a need for cultural mediators to facilitate the distribution, for example to interpret a language or regional dialect, it might also be necessary to process information about country of origin or ethnicity.

It is important that the NGO first of all determines if they even need to process the personal data in question to carry out the relevant purposes.

In our case, the NGO must determine if the processing of biometric data is necessary to provide aid through a CTP. This will be a discussion of the necessity of using biometric data versus other identification methods like ID cards. The interference in the data subjects personal life will also be important, as data minimization principle not only applies to the quantity of data, but also the

124 GDPR Article 5(1)(b)
125 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.315
126 GDPR article 5(c)
127 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 article 73

quality. A data processor cannot process data that causes a disproportionate interference in the subjects life, even if it is only one dataset.[128]

The word "necessary" is naturally understood as something that must be done, or something that is essential. Personal data should only be processed if it is not possible to fulfil the purpose by other means.[129] It must also be a reasonable and proportionate way of achieving the purpose. If the need to provide aid is very pressing, and the usage of biometric data like iris scans greatly increases the effectiveness of the distribution, this could be a good argument for the necessity of processing.

As discussed in chapter 6.3 and 7.1, the usage of biometric data cannot be proportionate in cases where the only reason for using biometric information is to ease the process of providing non-essential aid. In cases of essential aid that fall under the definition of "vital interests" it must however be within reason to say that the usage of biometric data is proportionate to the aim pursued. In such cases the usage of biometrics will make the process of providing aid significantly more effective, and the NGO in question will be able to provide aid to more people in need.

In relation to biometrics and new technology in general, it is also important to note that this technology is constantly being developed, and biometrics is being used more and more in society. As an example, the launch of face ID for Apple phones[130] was a huge step in biometric authentication. NGOs would be interested in keeping up with technological advances that could ease the identification process, and it is important to keep up with what is known to be common practice in society.

Refugees are generally in a more vulnerable position than the general public, and a high threshold for using new technology is a good way to protect them from being exploited. It can however be argued that NGOs should perhaps still be able to use new technology to ease identification and speed up the delivery of aid, even when such aid is not in the data subjects "vital interests". Technological development and necessity must be pitched against the right to privacy in this case.

In the case of providing aid through a CTP, additional data will be created through the program itself, such as credit transaction data.[131] This means that not only the collected data from the data subjects must be assessed.

The implementation of data minimization and proportionality can be hard to carry out. It is not always easy to know exactly what personal data is needed, and there is always a risk of collecting data that is not needed, and the assessment of what is "necessary" can be challenging. In this case it would be important that the NGO deletes any personal data that is proven to be unnecessary.

7.3 Security in accordance to article 5(f) and article 35

Another important aspect in relation to processing done by NGOs is security following Article 5(f). Data security is crucial, especially in the environments where humanitarian aid organizations often work. Poor information security can harm to the data subjects. The processing of any personal data must be done in a way that ensures "appropriate security", which includes protection against

128 Kuner et.al., *The General Data Protection Regulation: a commentary*, p.317
129 EDPB 4/2019 p.21 and GDPR recital 39
130 Apple Support, *'About Face ID advanced technology'*
131 ICRC *handbook on data protection* p.154

"unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."[132]

A number of the provisions in article 9 relating to special categories of personal data also require "safeguards" or "appropriate safeguards". Article 9 itself provides no further details on what this entails, but it is generally understood that these safeguards have to be designed based on the principles in article 5. The requirement is therefore closely related to the concept of security in accordance to article 5(f).

In C-342/12 (Worten) the CJEU pronounced that appropriate security means that only the "persons duly authorised" have access to the information in question.[133] This means that measures must be taken to ensure no unauthorized persons have access to the data in question.

There are several ways to do this, including physical, technological and organizational measures. Physical measures can include keeping physical data safe from unauthorized access by keeping them in a safe, restricting access to storage premises, and destroying printed copies when they are no longer needed.[134] Technological measures can include multi level password protection, designing systems in a secure way, reviewing and testing hardware, and replacing the identity of the data subjects.[135] Replacing identity is known as anonymisation[136] and pseudonymisation[137] of the data. In many cases anonymisation is not an option because of the need to continuously use the data as an identifier. Pseudonymity is therefore often a better option in humanitarian cases, as it means the people are still identifiable if the processor has the code to correctly connect data to the individual. Organizational measures can include ensuring that responsibilities are clearly allocated and ensuring that the personnel is familiar with the GDPR and the technological systems in use.[138]

In the case of processing biometric data in relation to a CTP, security will be very important. Because biometric data excels at identifying individuals, it is crucial that this data does not end up in the wrong hands, for example with opposing forces whose aim is to find and capture the refugees in question.

The CJEU has subjected processing data to special protection in cases where there is a high risk to the data subjects rights. This "risk of abuse" requires effective safeguards to ensure the legality of such processing.[139] Processing of biometric data on a large scale in relation to a CTP clearly pose a high risk of abuse. If the data is compromised, there is no way for the data subject to "reset" their biometric data like it would be possible to do with a password. Because of this, the NGO in question must undertake a data protection impact assessment (DIPA) to ensure that the processing is legal in accordance with GDPR article 35.

---

132 GDPR article 5(f)
133 Worten, C-342/12, paragraphs 28-29
134 EDPB 4/2019 p.27
135 EDPB 4/2019 p.27
136 Anonymous data refer to information that does not relate to an identified or identifiable person, or to personal data "rendered anonymous in such a manner that the data subject is not or no longer identifiable", see Recital 26
137 According to GDPR Article 4(5) "pseudonymisation" means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".
138 World food programme, '*Guide to Personal Data Protection and Privacy'* p.43
139 Breyer, C-582/14, paragraph 74

A DPIA contains a description of the envisaged activity, policy or data transfer involving the processing of personal data, a risk analysis of the rights of data subjects, the categories of personal data processed, in addition to the safeguards and measures taken to ensure the protection of the data.[140] A DIPA concerns both data protection and privacy rights, and fundamental rights and freedoms such as the freedom of speech. The obligation to carry out such an assessment is especially relevant in cases where the NGO makes use of new technologies that pose a high risk to the rights and freedoms of the data subject.

In addition, data subjects must be informed without undue delay about data breaches, when it is likely to result in a high risk to their rights and freedoms.[141]

7.4 Further processing

Sharing data is also a big part of humanitarian work, but it is also one of the riskiest aspects of data management. In many cases, humanitarian organisations might want to use already collected data for new situations if the need arises, or to share data with third parties. In the relation to CTP the NGO might need to receive data from another agency, and transfer information about the data subjects to a financial service provider.[142]

According to GDPR article 5(b) it is not legal to process data in a manner that is incompatible with the original purposes. It further follows from GDPR article 6(4) that there are three key mechanisms for further processing. The first case if the data subjects consents. In this case processing is legal. If a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) exists, the further processing is also legal. The third case is if a compatibility assessment demonstrates the compatibility of the further processing with the initial purpose. The third mechanism in particular is relevant for NGOs. Here the processor must take into account several points that can prove or disprove any link between the two processing operations. The proposed processing must be assessed on a case-by-case basis.[143]

In order to ascertain whether a purpose of further processing is compatible with the original purpose, the controller should take into account: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.[144]

Lastly, further processing or transfers for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes. If the secondary purpose fulfil these requirements the processing will still be legal.

---

140 GDPR article 35(7)
141 GDPR article 34
142 WFP, '*Guide to Personal Data Protection and Privacy*' p.56
143 WP203 p.21
144 GDPR recital 50

This is especially relevant for health data, and the recent years health data has been processed on a large scale in relation to statistics around COVID-19,[145] but could also potentially be relevant for biometric data in the future. Because biometrics are constantly developing, it's hard to say what long-term advantageous or disadvantageous effects they could have in a few years.

8. Summary

This thesis has explored four potential legal bases in GDPR article 9 for the processing of biometric data, specifically iris scans, in relation to providing aid through a CTP, as well as the connected data protection principles in GDPR article 5.

We have seen that the processing of biometric data raises some interesting questions related to the balance between the data subjects privacy rights and the NGOs need to process data to provide aid effectively. This is especially the case in relation to situations where consent is not valid, as we have seen can often be the case in aid situations, the legal basis for processing is not so easy to find.

The fact that the GDPR imposes strict restrictions on the usage of biometric data can lead to a dissonance between what's common in day-to-day life, and what can be legally used in an aid situation. The biggest difference in this case is that in day-to-day life, the data subjects will be able to consent to the use of biometric data.

It is however important to remember that people receiving aid from an NGO are in a position where their rights are already compromised. Even if biometric identification is commonplace, we still do not know the future implications of this technology, and using it in situations where the subject is not able to provide valid consent should raise several ethical questions for the controller.

If other legal bases than consent are to be used, it is therefore important to note that because of the asymmetric power balance between refugee and NGO, it might be impossible for the refugee to voice concerns or discomfort with the use of such technologies. If the NGO were to use consent, it would technically be possible for the data subject to refuse or ask for a different identification method. This would however be a flawed consent, and not an option under the GDPR.

The question is if we must allow the NGO to still be able to use technologies like iris scans when the subject is not able to consent based on their legitimate interest, or to carry out aid operations laid down in law, because of technological necessity and development. It is also important to balance out the need for efficient aid, and how common the practice in question is. If so, it is especially important to provide decent security measures in accordance to article 5(f).

145 See for example EDPB03/2020

9. Bibliography

Directives and regulations

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1), GDPR

Conventions and treaties

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ECHR

European Union, Consolidated version of the Treaty on the Functioning of the European Union, 7 June 2016, OJ C202/1, TFEU

UN General Assembly, Privileges And Immunities of The United Nations, 13 February 1946, accessed 1. December 2022 A/RES/22, available at: https://www.un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf

CJEU case law

Judgement of the Court of 10 October 1973, Variola, C-34/73, ECLI:EU:C:1973:101

Judgement of the Court of 21 March 2013, Kokott, C-431/11, ECLI:EU:C:2013:589

Judgement of the court of 30 May 2013, Worten, C-342/12, ECLI:EU:C:2013:355

Judgment of the Court of 17 October 2013, Schwartz, C-291/12, ECLI:EU:C:2013:670

Judgment of the Court of 13 May 2014, Google Spain and Google, C-131/12, ECLI:EU:C:2014:317

Judgement of the Court of 19 October 2016, Breyer, C-582/14, ECLI:EU:C:2016:779

Judgement of the Court of 20 December 2017, Nowak, C-434/16, ECLI:EU:C:2017:994

Judgement of the Court of 01 October 2019, Planet49, C-673/17, ECLI:EU:C:2019:801.

Judgement of the court of 11 November 2020, Orange Romania, C-61/19, ECLI:EU:C:2020:901

Judgement of the Court of 1 August 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, ECLI:EU:C:2022:601

Guidance and statements

A29WP Opinion 4/2007, Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP136, 2007. accessed 26. October 2022. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

A29WP Opinion 15/2011, Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, WP187, 2011. Accessed 21. October 2022. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

A29WP Opinion 3/2013, Article 29 Data Protection Working Party, Opinion 4/2007 on purpose limitation, WP203, 2013. Accessed 25 October 2022. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

EDPB, Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default (Version for public consultation) (2019), EDPB 4/2019, Accessed 1. December 2022. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

EDPB Guidelines 05/2020, European Data Protection Board, Guidelines 05/20 on consent under Regulation 2016/679, EDPB 05/2020, 4. May 2020. Accessed 1 September 2022. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, EDPB03/2020, accessed 1. September 2022, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

Case law from national cases

EDPB, *'Fine for processing students' fingerprints imposed on a school | European Data Protection Board'*, 2020, ZSZZS.440.768.2018, Accessed 8. September 2022, available from: https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

Books

Kuner, Christopher, Bygrave, Lee A., Docksey, Christopher, *The General Data Protection Regulation: a commentary*, Oxford 2020.

Schartum, Dag Wiese, *Personvernsforordningen – en lærebok*, 1. utgave. Bergen: fagbokforlaget 2020

Articles

Breckenridge, Keith "The Biometric State: The Promise and Peril of Digital Government in the New South Africa," Journal of Southern African Studies, June 2005, available at:

https://wiser.wits.ac.za/sites/default/files/Breckenridge%20-%202005%20-%20The%20Biometric%20State%20The%20promise%20and%20peril%20of%20digi.pdf

ComputerWeekly.com. *'Humanitarian Data Collection Practices Put Migrants at Risk'*. Accessed 1 September 2022. https://www.computerweekly.com/news/252492003/Humanitarian-data-collection-practices-put-migrants-at-risk.

Ensor, Charlie. *'Biometrics in Aid and Development: Game-Changer or Trouble-Maker?'* The Guardian, 22 February 2016, sec. Global Development Professionals Network. https://www.theguardian.com/global-development-professionals-network/2016/feb/22/biometrics-aid-development-panacea-technology.

EU, *'10 common principles for multi-purpose cash-based assistance to respond to humanitarian needs',* March 2015, accessed 28. November 2022, https://ec.europa.eu/echo/files/policies/sectoral/concept_paper_common_top_line_principles_en.pdf

Furl, Nicholas, Phillips, P.Jonathon, O'Toole, Alice J, *'Face recognition algorithms and the other-race effect: computational mechanisms for a developmental contact hypothesis'*, Cognitive Science, Volume 26, Issue 6, 2002, Pages 797-815, ISSN 0364-0213, Accessed 1. December 2022, Available from: https://www.sciencedirect.com/science/article/abs/pii/S0364021302000848

Human Rights Watch. *'UN Shared Rohingya Data Without Informed Consent*', 15 June 2021. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent.

'The Individualisation of War | Eye Scan Therefore I Am: The Individualization of Humanitarian Aid'. Accessed 14 October 2022. https://iow.eui.eu/2015/03/15/eye-scan-therefore-i-am-the-individualization-of-humanitarian-aid/.

Kaurin, Dragana. *'Data Protection and Digital Agency for Refugees'*, no. 12 (2019): 30. Accessed 1. september 2022: https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees/

Kuner, Christopher. '*International Organizations and the EU General Data Protection Regulation*'. SSRN Scholarly Paper. Rochester, NY, 1 February 2018. https://doi.org/10.2139/ssrn.3050675.

Kuner, Christopher. '*The GDPR and International Organizations'*. AJIL Unbound 114 (2020): 15–19. Accessed 19 September 2022, https://doi.org/10.1017/aju.2019.78.

The New Humanitarian. *'Eye Spy: Biometric Aid System Trials in Jordan*', 18 May 2016. https://www.thenewhumanitarian.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan.

The New Humanitarian. *'Eyes Wide Shut: The Challenge of Humanitarian Biometrics'*, 26 August 2015. Accessed 14 October 2022, https://www.thenewhumanitarian.org/opinion/2015/08/26/eyes-wide-shut-challenge-humanitarian-biometrics.

The New Humanitarian, *'Aid agencies rethink personal data as new EU rules loom'*, 18. January 2018, accessed 29. November 2022, https://www.thenewhumanitarian.org/2018/01/18/aid-agencies-rethink-personal-data-new-eu-rules-loom

Norwegian refugee council, *'First Distribution of Cash to Ukrainian Refugees | NRC'*. Accessed 16 October 2022. https://www.nrc.no/perspectives/2022/first-distribution-of-cash-to-ukrainian-refugees/.

Oostveen, Anne-Marie, and Diana Dimitrova. '*Iris Scanners Can Now Identify Us from 40 Feet Away'*. The Conversation. Accessed 25 October 2022. http://theconversation.com/iris-scanners-can-now-identify-us-from-40-feet-away-42141.

Rahman, Zara, Paola Verhaert, and Carly Nyst. *'Biometrics in the Humanitarian Sector'*, n.d., 22. Accessed 24. October 2022, https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620454/rr-biometrics-humanitarian-sector-050418-en.pdf?sequence=1

Tao et.al. (2012) Tao, Xunqiang, Xinjian Chen, Xin Yang, and Jie Tian. *'Fingerprint Recognition with Identical Twin Fingerprints*'. PLOS ONE 7, no. 4 (27 April 2012): e35704. https://doi.org/10.1371/journal.pone.0035704.

UNHCR Innovation. *'Using Biometrics to Bring Assistance to Refugees in Jordan'*, 30 August 2016. Accessed 24. October 2022 https://www.unhcr.org/innovation/using-biometrics-bring-assistance-refugees-jordan/.

Reports

International Committee of the Red Cross, '*Handbook on data protection in humanitarian action'*, 28.05.2020, accessed 14. October 2022, available from https://www.icrc.org/en/data-protection-humanitarian-action-handbook

World Food Programme, *'WFP Guide to Personal Data Protection and Privacy'*, June 2016, Accessed 11. November 2022, available from https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Dictionaries and web pages

Apple Support, '*About Face ID advanced technology'*, accessed 1. December 2022, https://support.apple.com/en-us/HT208108

GDPR.eu. (website) '*What Is GDPR, the EU's New Data Protection Law?*', 7 November 2018. accessed 19. september 2022, https://gdpr.eu/what-is-gdpr/.

ID, IRIS (blog) '*What Is the Difference between Iris Recognition and Retinal Scanning?'*, 26 September 2003. Accessed 28. October 2022 https://www.irisid.com/what-is-the-difference-between-iris-recognition-and-retinal-scanning/.

Law Insider. *'International Organisations Definition'*. "international organisation", accessed 28 October 2022. https://www.lawinsider.com/dictionary/international-organisations.

National Geographic society, '*International Organization | National Geographic Society*'. "international organisation", accessed 28 October 2022. https://education.nationalgeographic.org/resource/international-organization.

OECD Glossary of Statistical Terms, '*International organisations Definition*', "international organisation", accessed 3 October 2022, https://stats.oecd.org/glossary/detail.asp?ID=1434

Practical Law. *'International Organisation'*. "international organisation", accessed 28 October 2022. http://uk.practicallaw.thomsonreuters.com/w-014-8185?transitionType=Default&contextData=(sc.Default)&firstPage=true.

UNHCR, '*Internally Displaced People*', accessed 22 October 2022, https://www.unhcr.org/internally-displaced-people.html

UNHCR, '*What is a refugee*', accessed 22. October 2022, https://www.unhcr.org/what-is-a-refugee.html