Symphonies of Personal Data Protection: Humanitarian Organizations on the Stage

Symphonies of Personal Data Protection: Humanitarian Organizations on the Stage

Tetiana Avdieieva

Kyiv, 2023

The **aim of the study** is to analyze the personal data practices of organizations performing humanitarian functions as part of the armed conflict (Russian aggression in Ukraine), to assess the potential risks of policies and practices of such organizations and possible solutions to enhance data protection in wartime.

General editor: Tetiana Avdieieva
Author team: Tetiana Avdieieva
Literary editor: Maryana Doboni
Design/layout: Inna Smuchok
Translation: Rostyslava Martyn

The research “Symphonies of Personal Data Protection: Humanitarian Organizations on the Stage” was prepared within the project “Documentation of war crimes committed by the Russian Federation” with financial support from the National Endowment for Democracy, USA. Views of the study's authors do not necessarily reflect the official position of NED or the US Government.

Analytical research/General ed. Avdieieva T. - Kyiv, 2023 - 54 p.

TABLE OF CONTENTS

INTRODUCTION

War is the ultimate threat to the right to life and health, and in the case of the Russian invasion, also to the right not to be tortured. In the face of such fundamental things, everything else becomes less important. For example, who will care about not being able to go to a protest, hold a religious ceremony or write a post about what is going on outside if missiles are flying overhead? However, there are actually some things that, albeit indirectly, have a significant impact on security. Among them, one of the key issues is the protection of personal data. Thus, data leaks can lead to persecution of vulnerable groups, detention of activists, and even mass execution of those affiliated with the state structures (as was repeatedly the case in the Russian-occupied territories)

During armed conflicts, personal data play an extremely important role both for the protection of civilians (e.g., providing humanitarian aid), planning operations, predicting the development of military operations (needs roadmapping), and emergency communications (contacting relatives or organizations that ensure evacuation, etc.). In general, studies show that the following sources of sensitive information are most often used during an international armed conflict:

- **Intelligence or surveillance data,** which predominantly provide a general understanding of trends in the movements of individuals (unless special biometric identification technologies are used, which provide a wider range of capabilities to the authorities collecting such data);

- **Open data** contained on social media (e.g., the actions of the infamous Clearview AI), blogs, and media (interview responses, targeted studies, etc.). Such information, although accessible, helps, for example, to spread enemy propaganda, because it facilitates better audience study or allows the identification of detained persons;

- Information provided **in response to surveys, SMS, hotline, etc.** Such data is used to anticipate needs and can rarely help to identify individuals (because the purposes of collecting such data are somewhat different). However, given that the data is technically stored anyway, there are risks of it being leaked or reaching warring parties;

- **Information provided by individuals themselves when receiving humanitarian assistance** (the source of the largest amount of data collected). Such information may contain both mandatory data and so-called residual data that can be used for profiling or tracking an individual. This is why such data should be handled with extreme caution

In response to this extensive processing of personal data from various sources, back in 2017, the International Committee of the Red Cross (hereinafter referred to as ICRC) noted the need to strengthen protection for messengers and social media, and in 2018, it emphasized that online payment applications needed special data protection rules. Subsequently, in 2019, the ICRC developed Policy on the Processing of Biometric Data with recommendations on how to ensure neutrality, impartiality and independence when processing civilian data during armed conflict. Finally, in 2021, an updated Handbook on Data Protection in Humanitarian Action was released, designed to answer most (or all) of the current challenges in the protection of sensitive information. All the above documents qualified data leaks, negligent processing and storage as the main challenges that both organizations and users are now facing. A little later, we will find out whether these recommendations are in line with the real context in which humanitarian aid providers operate during modern armed conflicts.

However, as practice shows, personal data is most often used to provide humanitarian aid: one-time or regular financial support, provision of certain medicines or basic necessities, granting refugee status, status of a person in need of temporary protection, granting temporary asylum and the like. Therefore, it is this area that requires the most careful analysis. International

organizations, in particular, collect and store personal data on displaced persons to help them re-establish ties with their relatives after the end of an armed conflict. This practice is not new and had already been used during the conflict in South Sudan and after the Ebola epidemic in the Democratic Republic of Congo.

A large amount of data is also collected by regular humanitarian assistance providers, in particular for cost projections. For example, the Swedish Migration Agency analyzes "big data" to establish the number of migrants or asylum seekers. However, along with data storage, data representation has become a problem: sometimes not all individuals can get help because of a lack of information about the necessary medicines, food or money. This problem does not concern the fact of data collection itself, but its transfer between different organizations at local, regional and international levels.

In order to avoid such situations or at least to reduce the typical risks, international and regional organizations whose regular function is to provide humanitarian assistance have developed a number of recommendations on the proper handling of personal data during armed conflicts. Although mostly quite general, they serve as an excellent mapping of the challenges, risks and weaknesses of data protection policies that arise in practice. Human rights institutions such as the UN Special Rapporteur on the Right to Privacy have noted that all risks should be contextualized. For example, although humanitarian organizations assure that they anonymize the data collected, there is always the possibility of re-identification of individuals through a combination of multiple databases. Therefore, in addition to declarative standards, it is also necessary to take into account the practical challenges that arise with the development of technology and the transition of armed conflicts to a new level. After all, while trying to help, organizations can sometimes do more harm than help, leaving people as targets of persecution, allowing their data to be used for manipulation, military operations planning or information attacks.

Russia's full-scale invasion in February 2022 caused a significant need for humanitarian assistance for internally displaced persons (hereinafter referred to as IDPs), children who have lost parents/guardians as a result of armed aggression, vulnerable populations and many other categories of Ukrainians. In order to avoid abuse and even distribution of available assistance, state and local authorities, as well as international and national humanitarian organizations, are forced to record the identity of those to whom such assistance is provided.

Any records that allow for identification automatically involve the collection and processing of personal data. Rules for handling confidential information are stipulated by both international acts (hard and soft law) and national regulation (the Law of Ukraine "On the Protection of Personal Data", clarifications of Ukrainian Ombudsman on data protection during martial law, etc.). In accordance with the Law of Ukraine "On Humanitarian Aid", organizations that provide it, independently determine the scope of personal data, purposes, conditions and terms of their processing and method of protection. Also, the obligations imposed by the law include the creation of a database of personal data of acquirers and rules for accessing and processing data in such database, election of a person who will supervise such processes, etc.

One would wonder, what could go wrong in the presence of detailed guidelines? However, even this did not save the Ukrainian information space from scandals: for example, the United Nations Children's Fund (hereinafter referred to as UNICEF) was accused of illegal and disproportionate collection of data of Ukrainians who received monetary assistance from the organization (violation of the principle of obtaining consent). It is worth noting that the accusations were later refuted by the Vox Ukraine fact-checking team, which proved that there were no violations by the international organization in the matter of personal data protection.

At the same time, this case drew public and, most importantly, human rights defenders' attention

to the issue of limiting and protecting privacy during martial law. In particular, the pressing issues include the legal and technical ability of organizations providing assistance to vulnerable populations to protect the personal data collected and to ensure their inaccessibility to the aggressor country, in particular in the occupied regions. Given the sharp increase in the number of humanitarian organizations since February 24, 2022 (five-fold increase compared to the situation before the full-scale invasion), there is a concern about whether the newly established organizations have adequate policies on data processing, including sensitive information. Thus, in 2022, the focus was predominantly on the provision of assistance itself, while compliance with data protection procedures and proper data storage were put on the back burner. In this context, for example, the relevant question is whether international organizations, such as UNICEF, the World Food Program and the ICRC, share the collected data with their offices in the aggressor country (provide access to a common database).

To answer these and many other questions related to the collection of personal data by humanitarian organizations, UMDPL conducted a comprehensive study on the compliance with national and international standards. **The aim of the study** was to analyze the personal data practices of organizations performing humanitarian functions as part of the armed conflict (Russian aggression in Ukraine), to assess the potential risks of policies and practices of such organizations and possible solutions to enhance data protection in wartime.

The key objectives of the analytical study included:

- Collecting information on the existing personal data protection policies of organizations performing humanitarian functions in the context of the war in Ukraine;
- Identifying dangerous or illegal practices of personal data collection, processing, storage or transfer within the humanitarian assistance;
- Assessing the riskiness of such practices and proposing legal and technical options to address the problem of insufficient protection of personal data.

As part of the study, the authors used **data** from open sources of information, having studied, in particular, the practice of international and national courts, statistical data on the websites of organizations, results of social surveys and indices of compliance with data protection rules, targeted interviews and surveys, materials from Ukrainian and regional media, studies of human rights organizations, as well as responses to information requests from national and international organizations and experts. If we had to use materials from unofficial sources, we cross-checked the accuracy of information in other sources; also, the text mentions the lack of confirmation of data if it was available in only one source / several sources that for certain reasons cannot be considered reliable or objective.

As a result of the study, recommendations were developed for international, foreign and Ukrainian organizations to improve personal data protection policies when providing humanitarian aid and performing other humanitarian functions. It also provided a number of recommendations to other stakeholders that affect the protection and transfer of personal data when providing humanitarian assistance by the respective organizations (e.g. state, local self-government bodies, beneficiaries etc).

SECTION I.
Martial Law Plays First Fiddle

Undoubtedly, armed conflict is a deviation from the usual protection procedure, restrictions and exercise of human rights. War generates new risks that often shift the emphasis in balancing rights. Thus, the protection of the right to life is becoming more urgent (because the number of threats is increasing), while the right to freedom of peaceful assembly, the right to freedom of movement, or voting rights are subject to greater restrictions. This shift in paradigm and priorities during an armed conflict is enshrined in international and national law. In particular, the state has the right to derogate from its obligations under international treaties in case of emergencies (natural or man-made disasters, epidemics, social unrest, etc.) or the outbreak of war. The basis for this is a decision to declare a state of emergency or martial law, respectively, adopted at the national level.

Such special legal regimes allow national authorities to better protect fundamental rights and balance interests according to pressing needs and risks which national governments are best informed of. In fact, both regimes involve an expansion of state discretion and the ability to make certain decisions not contemplated by the law applicable in times of peace. However, such discretion is not unlimited: international law and national legislations contain safeguards against possible abuses, in particular to avoid regimes becoming authoritarian. That is why, before assessing whether humanitarian organizations comply with personal data protection rules, it is necessary to find out which rules are applicable both at the level of the state and of private actors.

International standards and derogation regime. The possibility to derogate (or prohibition on derogation) from obligations under international conventions is provided for separately by each treaty. Two documents ratified by Ukraine – the International Covenant on Civil and Political Rights (hereinafter ICCPR) and the European Convention on Human Rights (hereinafter ECHR) – are relevant in the context of Russian aggression. Each of them has a separate mechanism for activating the derogation regime in case of emergency, as well as standards to be adhered to when imposing additional restrictions for the period of such regime. Let's find out what their features are.

Article 4 of the ICCPR provides for a mechanism for derogation from Covenant obligations in the event of an emergency which "threatens the life of the nation and the existence of which is officially proclaimed". Although the wording is rather vague, Article 4 sets out several criteria for the validity and legality of derogation (which, however, are still general and vague)

Conditions under which derogation from obligations under Article 4 of the Covenant is **valid**:

- A state of emergency in which the life of the nation is threatened;
- Derogation is made within the limits "required by the urgency of the situation";
- Derogation is compatible with other obligations under international law;
- Derogation does not result in discrimination solely on the basis of race, religion, color, sex, language or social origin;
- Derogation does not concern the right to life, the right not to be subjected to torture, the right to be protected from slavery, the right not to have one's liberty restricted because of inability to fulfill obligations, the right not to be punished without law, and the right to freedom of thought, conscience and religion;
- The state has informed the UN Secretary General of the measures taken and the reasons for them in a timely and complete manner.

The provisions of Article 4 are interpreted in General Comment No. 29 to the ICCPR. Thus, the UN Human Rights Committee emphasizes that derogations are temporary and exceptional in nature [§ 2]. In particular, this means that a state is unable to address the protection of fundamental rights or interests through laws already in force. The Committee also noted that when drafting derogation, the state must clearly list possible additional measures and justify the necessity of each of them to protect a legitimate interest. Otherwise, it would violate the principles of necessity and proportionality. The Comment also contains an additional duty for the state (which is not mentioned in Article 4) to restore the violated rights or to make reparation for damages.

As the ICCPR applies to a slightly larger number of countries than the ECHR (which we will discuss a little later), the number of derogations over the history of the Covenant is quite significant. In 2020 alone, the UN Secretary General received 27 derogation reports in response to the pandemic. Due to the wave of derogations, the UN Human Rights Committee issued a statement calling for non-derogation in cases where it is possible to protect rights and freedoms through the normal mechanism of limitations under the core articles of the Covenant. In addition, derogation reports from most countries have been assessed as very vague and unclear, with a lack of adequate justification for additional restrictions on rights.

The system provided for by the ECHR is somewhat different: Article 15 establishes not only a clear mechanism for derogation in times of emergency, but also certain conditions for its validity. Unlike the ICCPR, the Convention explicitly mentions war as grounds for extending state discretion and changing the lens through which human rights are assessed. It also provides for certain other requirements.

The conditions under which derogation under Article 15 of the Convention is **valid:**

- War or other public danger which threatens the life of the nation;
- Derogation does not concern the right to life (except in cases of death due to lawful hostilities), the right to the prohibition of torture and slavery, the right not to be punished without law;
- Derogation is made within the limits ”required by the urgency of the situation”;
- The state has informed the Secretary General of the Council of Europe of the measures taken and the reasons for them in a timely and complete manner.

Formal compliance does not ”give a free hand” to the state in the matter of restricting rights. Although Article 15 of the ECHR had not been used much in the past (only a few countries have done so), after the pandemic many countries started to use this mechanism. And this gave rise to quite a wide practice in the interpretation of the provisions of Article 15, as well as the definition of the limits of such state discretion by the European Court of Human Rights (hereinafter referred to as ECtHR), in particular with regard to the restriction of the right to privacy and protection of personal data.

Importantly, until February 24, 2022, no state had **derogated on the basis of a state of war**. This means that comparisons with other precedents should be made very cautiously, as neither a pandemic, nor social unrest, nor probable terrorist acts are comparable to an armed conflict in terms of intensity and danger. Therefore, when analyzing the ECtHR’s practice, one should take into account the general principles of interpretation of Article 15 rather than draw specific parallels with the circumstances of the cases.

First of all, the ECtHR considers the derogation regime to be an exceptional mechanism. In Ireland v the United Kingdom, the Court noted that it first assesses whether the restriction is in conformity with the basic provisions of the ECHR, and only when inconsistency is established

does it analyze whether the derogation was proper [§ 191]. A logical conclusion can be drawn from this: not every derogation can be necessary and proportionate, even if formal requirements about a report or public danger exist. In assessing necessity and proportionality, the Court considers the following criteria:

- Sufficiency of ordinary laws to protect a legitimate interest;
- Ability of the measures to help in an emergency (to protect a particular interest);
- Clarity and predictability of derogations, the specific list of measures that can be applied for such a period;
- Revision of derogations over time;
- Loosening of measures over time or in certain regions;
- Availability of safeguards against abuse;
- Other criteria that depend on the nature of the limited right.

While the validity of the derogation report is already assessed by the Court when a precedent arises (when a complaint is brought before the ECtHR), states must also take these criteria into account when drafting derogations and determining their scope. In particular, according to A. and Others v the United Kingdom, restrictions must be lawful at the time of their introduction but must also take into account further developments, such as a decrease in the intensity of riots, etc. [§ 177].

Assessing necessity and proportionality has never been a simple task, as scholars have noted since the early 21st century, assessing cases against the United Kingdom, Greece and Turkey. However, it is important for a state to initially establish a predictable legal regime in order to avoid unnecessary lawsuits from both its own citizens and foreigners affected by such restrictions. This is also relevant in the case of Ukraine, so it is worth analyzing the restrictions mentioned in the communication of derogations from the ECHR and the ICCPR (they were sent in one document).

After the start of the full-scale invasion, Ukraine sent a communication regarding derogation from obligations under the ECHR and the ICCPR.. The communication was received on February 28 and registered by the UN Secretary General on March 1, 2022. Subsequently, on March 4, 2022, the Permanent Mission of Ukraine sent a supplement to the report clarifying the scope of the derogation.

The communication itself contains references to the presidential decree on the imposition of martial law and the law by which it was approved. The communication also contains a list of constitutional rights, restrictions of which are provided for during the period of martial law, and corresponding articles of the ICCPR and the ECHR. The list is followed by an almost verbatim translation of the decree with possible forms of restrictions on the mentioned rights. However, the state did not provide justifications for why exactly such forms of restrictions are planned to be applied. In contrast to the reports of many states during a pandemic or social unrest, Ukraine did not indicate clear limitations on certain rights (e.g., freedom of expression or privacy), noting in general terms the possibility of limiting them. Subsequently, the lack of justification was also noted in the study by Council of Europe experts who assessed the legality of derogation.

However, let us assume that the reference in the communication itself to the legislation on martial law and acts of the national authorities is sufficient. In this case, all roads lead to the

decree of the President of Ukraine on the introduction of martial law and accompanying acts of the government, so it is high time to find out how clear and predictable these documents are.

Martial law in Ukrainian legislation. Article 64 of the Constitution of Ukraine provides for the possibility of restricting certain rights under martial law or state of emergency. The procedure for imposing martial law and its peculiarities are regulated by the Law of Ukraine "On the Legal Regime of Martial Law". Among the possible measures that relate to the right to privacy, Article 8 provides for the possibility of checking documents, belongings and dwellings, and allows for the implementation of "other measures provided for by the norms of international humanitarian law", which sometimes also refer to the transfer of personal data. Otherwise, the Law provides a general framework, while specific restrictions should be established directly by the acts by which martial law is imposed.

On February 24, 2022, after the beginning of a full-scale invasion, based on a proposal of the National Security and Defense Council of Ukraine, the President issued a decree "On Imposition of Martial Law in Ukraine". According to the decree, the Cabinet of Ministers of Ukraine was to develop a plan to ensure and implement martial law measures. After the decree was approved by the relevant law, the government developed such a plan, but there were only a few lines in it focusing on human rights, and even fewer focus on privacy. Thus, the action plan simply duplicated the provisions of the law on martial law, authorizing law enforcement and military bodies to carry out document checks of persons and, if necessary, to inspect the belongings, vehicles, luggage and cargo, offices and housing of citizens. At the same time, Article 25 of the Law of Ukraine "On Protection of Personal Data" indicates that derogations from the provisions of the articles on data processing may be made only if they are expressly provided for by other legislative acts. If such restrictions have not been "activated" in the manner prescribed by law, the general regime of personal data processing will be applicable.

Are special restrictions imposed on the right to personal data protection? At the level of a presidential decree or an action plan developed by the government – no, of course not, except for the possibility to check a person's ID, personal belongings and housing. This means that restrictions on the right to privacy that go beyond such measures should be stipulated by laws and comply with the general requirements of the Law of Ukraine "On the Protection of Personal Data". We will evaluate these regulations when we analyze the rules under which humanitarian aid is provided and data transfers take place.

If the derogation regime is primarily about the state, its discretion and obligations to justify restrictions, why is it important to talk about it when analyzing the activities of humanitarian organizations?

- First, derogation is not only a state's ability to further restrict rights and the obligation to explain why such restrictions are imposed, **but also a special legal regime in a particular territory**. It applies to all actors operating in such a legal field and imposes restrictions even on those who are not expected to be subjected to them. For example, humanitarian organizations may sometimes be forced to disclose beneficiary data under a simplified procedure at the request of law enforcement agencies if there is a suspicion of a violation of the law. However, as the analysis of imposed restrictions shows, there are no such requirements in Ukraine.
- Secondly, **simplified rules are sometimes introduced for humanitarian organizations**, because their activities become more relevant in times of crisis, such as war or natural disasters. In such cases, they may collect more (or on the contrary) less data, which will have an impact on the rights of beneficiaries.

However, derogation and martial law are only a general framework. In addition to them, there is a whole set of international and national standards applicable to humanitarian organizations and recipients of humanitarian aid. Before analyzing the policies and practices of such organizations in Ukraine, let us find out what standards have been developed by advanced international bodies.

SECTION II.
Orchestra of International Standards

Speaking about international standards of personal data protection, European experts most often mention two documents – General Data Protection Regulation (hereinafter referred to as GDPR), which operates at the EU level and is applicable to companies falling under the jurisdiction of the EU, and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereinafter referred to as Convention 108+), which is applicable to the parties that have ratified it (mainly member states of the Council of Europe). Both instruments deal with the general standards in the field of data protection, focused mainly on peacetime. There are almost no specific provisions on data processing during a state of emergency; however, it is this framework regulation of data processing that is referred to in all specific recommendations for humanitarian organizations. Therefore, before looking at whack-a-mole guidelines, let's find out the general standards in the field of data protection.

Convention 108+. This document is quite general and somewhat outdated compared to the GDPR. For example, the Convention itself entered into force back in 1981, and the latest updates – the Additional Protocol – were signed in 2001. That is, most of the modern ways of data processing, including through systems controlled by artificial intelligence, are not taken into account in the provisions of this act. However, the following principles are undoubtedly relevant in the field of data processing for humanitarian purposes:

- Legality of data collection and processing;
- Compliance of data processing with the purpose and aim of data collection;
- The principle of minimization (non-redundancy) of data collection in relation to the purposes of data processing;
- Accuracy and timely update of outdated data;
- Limitation of storage periods for the purpose of data processing.

It is the Convention 108+ that laid down these principles of personal data processing along with other important principles, such as data security in legal and technical spheres, guarantees for the personal data subject (notification of the fact of data processing, possibility of data deletion or rectification, use of legal remedies in disputed cases, etc.). In addition, Convention 108+ established another important rule – the existence of a special category of data (sensitive data).

> Personal data on race, political views, religion or other beliefs, data concerning health or sexual life cannot be subjected to automated processing unless legislation provides for appropriate safeguards. That is, such data is **sensitive data.**

Importantly, the Additional Protocol establishes the o**bligation to establish supervisory authorities** to ensure compliance with the rules on personal data processing and protection. Although there are no detailed requirements for such a supervisory authority, this standard has become an additional safeguard against abuses in the field of personal data protection. However, Convention 108+ is still an overly general and outdated act, the provisions of which have been largely clarified and supplemented by other regulatory documents. GDPR has become one of them.

GDPR. The EU regulation, which came into force in 2018, is much more detailed in its approach to the standards of personal data protection. Thus, some of the principles included the requirements for the consent of the subject to the processing of information about them. In particular, GDPR specifies that the consent must be free and informed, i.e. the person must be aware of what data is collected and for what purpose, to whom it may be transferred, etc., as well as have the right to withdraw consent to data processing if necessary. In addition, the document also specifies the **grounds for processing sensitive data**, they can be summarized as follows:

- Predictability of data processing directly at the level of law;
- Data processing based on the subject's consent;
- Processing is necessary to protect the vital interests of the data subject;
- Processing is carried out by non-profit organizations due to the purpose of their legitimate activities;
- Processing of data that is publicly disclosed by the data subject;
- Processing necessary for legal proceedings;
- Processing necessary for medical purposes or for the protection of public health;
- Processing is carried out for public interest, scientific, statistical or historical purposes.

In other cases, the processing of sensitive data is prohibited. However, among the specified grounds are those that allow the processing of data on origin, gender (sex) or sexual orientation for the provision of humanitarian assistance, such as the consent of the individual or the protection of their vital interests or the public interest (Recitals 46, 73 and 112 of the GDPR expressly provide for this possibility). Such a regime is much safer, as it restricts organizations from processing sensitive data without due justification, and also brings them to the principle of data minimization: should it be possible to provide assistance while obtaining less data, it is better for the organization to use this option.

Additionally, GDPR establishes requirements for a national data protection regulator – a state body that will develop technical standards and oversee compliance by other government agencies, private organizations and companies. Importantly, responsibilities are also placed on the companies themselves: they should create an institution / appoint a **person responsible for monitoring compliance with the legislation on personal data protection.**

GDPR also introduces a number of **new rights** for personal data subjects:

- The right to be informed;
- The right to access their personal data;
- The right to have incomplete or inaccurate information corrected;
- The right to have information erased (right to be forgotten);
- The right to object to data processing;
- The right to withdraw consent;
- The right to opt-out of automated data processing.

The GDPR therefore sets out clearer requirements, and many of these are explicitly applicable to cases of data processing when providing assistance. For example, when it comes to sensitive

information, its storage and deletion. The Regulation also extends the rights of the data subject and allows them to request deletion of data and information update if it is outdated. The ability to require data processing by a live person rather than an automated system is also important. This is relevant in cases where border guards or assistance providers identify individuals using facial recognition systems that have a high error and inaccuracy index. In general, any automated data processing can lead to significant harm, so the additional safeguards are a positive step, especially for areas such as humanitarian aid (where GDPR is clearly applicable).

What about more "humanitarian" standards? In addition to general documents, sector-specific standards are also relevant – mainly in the field of humanitarian aid and personal data protection, they are soft law in nature. That is, these standards are recommendatory rather than mandatory. Nevertheless, they are issued by specialized organizations that are reputable among the majority of conscientious institutions. In addition, they contain the already mentioned general standards adapted to the context of armed conflicts and emergencies. Therefore, let us consider the specific standards applicable to data protection in humanitarian assistance.

A fundamental document is the ICRC's Handbook on Data Protection in Humanitarian Actions. Its premise was the need to reconcile the legal regimes of human rights law and humanitarian law, which are applied simultaneously during armed conflicts. While the first steps had already been taken in developing the GDPR Recitals and recommendations at the level of the UN, the Council of Europe and other regional bodies, they mostly lacked proper contextualization and assessment of the risks inherent in handling data during conflicts. Therefore, leading experts have produced a 300+ page document that defines the key principles for handling personal data during humanitarian actions (both during direct provision of humanitarian aid and during evacuations, search for missing persons, when during with prisoners of war, etc.). Furthermore, the Handbook has an advantage – it can be applied regardless of the specificities of national regulation. When assessed in the context of this study, the standards described below are applicable both to international organizations providing humanitarian assistance in Ukraine and to national human rights, charitable and humanitarian organizations.

Principles. Just like any other document that aims to regulate social relations from a legal point of view, the introductory part of the Handbook begins with the principles of working with data during humanitarian actions. Unlike the GDPR, the Handbook does not just list the principles, but also details them and provides examples of their application in practice. What principles does the Handbook mention?

- **The principle of legality of working with personal data.** In addition to compliance with the requirements of international instruments (such as GDPR or Convention 108+) and national standards of the state in which organizations provide humanitarian assistance, according to the ICRC, this principle also covers transparency and predictability of the processes that humanitarian organizations should ensure for personal data subjects. Thus, a person applying for humanitarian aid must understand what will happen to their data and according to which legislation the processing will be carried out.

- **The principle of limiting data processing to a specific purpose.** Unlike other, more general documents, the Handbook explicitly states seven purposes for which data may be processed in a humanitarian context. In particular: direct provision of humanitarian aid; reunification of families whose members were separated as a result of the armed conflict; providing protection to persons and buildings that have a protected status in accordance with human rights law and humanitarian law; healthcare; protection of homes and access to water; identification of persons and their integration into national systems (for example, through the institution of asylum or refugee status). The list of purposes is exhaustive.

- **The principle of proportionality.** Collection of personal data in the amount that is exhaustively required to perform the functions of a humanitarian organization. At the same time, the Handbook offers several rational clarifications, for example, it cites cases when the

purpose of data collection is quite broad at the time of its collection due to the emergency of the situation. In such situations, the principle of proportionality requires the deletion of excessively collected data as soon as the organization becomes aware of the fact that such information is not necessary for the performance of humanitarian functions.

- **The principle of data minimization.** This principle is to some extent derived from the principle of proportionality, however, it is more focused on protecting the subject from excessive collection of data that may be generally relevant to the achievement of the objective. For example, there is a requirement for a humanitarian organization to carry out its functions by collecting the minimum possible amount of personal information about aid recipients. For instance, there are often discussions about the legality of collecting biometric data from refugees (retinal scanning, facial recognition, etc.), which is not carried out by border guards when these persons are entering the country, but by humanitarian organizations when providing aid. In fact, this principle runs through all activities and includes not only limited data collection, but also limitation of their storage periods, timely deletion of outdated or unnecessary data, anonymization of data, etc.
- **The principle of maintaining proper data quality.** In particular, organizations should ensure that data is current and properly updated. This is important in cases where humanitarian aid is provided over a period of time, such as a year, when people may change their last name, get married or when other events occur that affect the receipt of support and its scope.
- **The principle of safety and security of data.** Organizations that provide humanitarian assistance ensure that personal data will be properly protected technically in matters of storage and access to information, and will not be illegally transferred to third parties, having an appropriate level of legal protection.

Many additional principles are also mentioned in other soft law documents. For example, the Interagency Standing Committee in the Operational Guidelines for Data Responsibility in Humanitarian Activities separates the principles of processing personal data and information that is collected during the provision of humanitarian assistance, but is not personal data. Thus, for non-personal data, the Commission singles out the principle of **responsibility and accountability** (for organizations that process data), **confidentiality** (for other departments of the organization, third parties and the state), **data security**, human-centeredness in data processing and collection processes, cooperation between partners in providing humanitarian aid (for the state, civil society, international organizations, etc.) and several derivative principles (such as data deletion). However, it is worth noting that the mentioned principles are quite applicable to the processing of personal data: it is hard to imagine that handling information involving the identification of individuals would not be in line with the principle of confidentiality, security or responsible data handling.

A similar list was provided by the UN Office for the Coordination of Humanitarian Affairs, which in the Guidelines for Responsible Data Work emphasized the need to focus the processes of working with personal data in the humanitarian sector on the human rights protection. In addition, it categorized all principles according to three main areas:

Safety	Ethics	Efficiency
Legal and technical security of data at all stages of their processing	Adherence to the principles of data ethics and work ethics in the humanitarian sector	Ability to achieve the purpose of data collection

The entire approach of UN institutions to the protection of personal data is built on these three fundamental pillars. For example, during the work on a separate Data Strategy during the COVID-19 pandemic, emphasis was placed on data security, data privacy and effective management of data circulation within UN subsidiary institutions. A similar approach can be seen in the UN Secretary-General's Roadmap, which emphasized the need to ensure data security and strengthen inter-agency cooperation in this area.

As can be seen from the analysis of the main recommendation documents in this field, intergovernmental and non-governmental organizations are "on the same page" regarding the principles of working with personal data. In fact, the work comes down to the promotion of responsible attitude towards the work with personal data among the organizations performing humanitarian functions. The development of this attitude is possible thanks to the development of universal principles. The legality of work with personal data is assessed through their lens, in particular, the development of general policies. However, the development of policies and the assessment of risks and threats to human rights is not the final point in this story. What is more important here is the practical application of such policies to real-life scenarios.

Data collection does not always involve writing the full name and passport number on a paper form. Today, digital technology is increasingly used: data collection may take the form of facial recognition by an automated system, collection of cookies on a website where the beneficiary must register, uploading documents to shared databases, etc. In such cases, it is important for aid organizations to ensure that they have legitimate grounds for collecting data. One of the most common grounds for processing personal information is an individual's consent. However, even this has separate ethical and legal requirements.

Person's consent. The ICRC Handbook outlines the characteristics of consent to the processing of personal data that make it valid. In particular, the individual's consent must be:

- **Informed.** The person must be informed about the type of personal data being collected for humanitarian assistance, the purposes for which it is being collected (why this particular data is needed), the period and procedure for storing the personal data, the grounds for transferring the personal data to third parties (e.g. other organizations or the state), and the conditions for correcting and deleting outdated and inaccurate data. It is not enough to simply say that personal data is being collected, the individual must fully understand all the processes in which their personal data will be involved. Only then is consent informed.

- **Clear.** Ideally, consent should be provided in writing on a special form that also contains the privacy policy of the humanitarian aid organization. This way, in the event of a dispute, it can be established whether consent was actually provided. If it is not possible to obtain consent in writing, it can be videotaped with the permission of the person giving consent. However, it must be understandable and clearly reflect the person's position.

- **Timely.** Consent must be provided before humanitarian assistance is received. It is a violation to provide assistance with appropriate processing of personal data, after which the organization requires consent for such processes, in particular, because the individual will not be able to object to or prevent the use of their data or refuse assistance.

- **Free.** Consent is considered free if the individual can opt out of receiving assistance. For example, a person may consider the amount of data processed to be excessive or may not wish to leave certain information to a humanitarian organization. In addition, a person has the right to refuse from automated data processing. In this case, he or she must be offered data processing by a live person. Also, the individual must be aware of all the consequences of the collection and processing of their data.

- **One that takes into account the vulnerable situation of the individual.** The social, cultural and religious situation of the individual should be taken into account when collecting personal data. The process of collecting personal data should be done in a way that respects the characteristics of the individual, taking into account:

  - illiteracy, presence/absence of disability, age, health status, gender and sexual orientation;
  - location of the person (such as a temporary shelter, a place of restriction or deprivation of liberty, a remote place with limited communication, etc.);
  - the language of communication, ignorance of the legal features of the country where it receives assistance, etc. (for example, foreign and international organizations must make sure that the population of the region where they work understands the
  - meaning of data processing);
    the fact of belonging to a political, ethnic or social minority/majority;
  - potential impact of technologies on the individual if they are flawed with respect to, for example, people of color, based on gender or other characteristics (as is often the case with facial recognition technologies).

- **Revocable.** At any stage of data processing, an individual has the right to withdraw consent and request the deletion of any information about them. At the same time, they must be notified of the consequences of withdrawing consent. The same rules apply to consent also apply to consent withdrawal: it should not be made under pressure from third parties, it should be informed and timely. In such cases, many questions arise regarding systems where consent is provided by checking a box on a website. On the one hand, consent is considered free and informed, on the other hand, is it possible to withdraw it and demand the termination of data processing if the website or form has no technical support or connection to a live person? The situation is similar with cookie banners that collect information about online activity.

And while there are quite a few other grounds for lawful data processing besides consent, most of them depend on interpretation of the circumstances rather than on the behavior of the data subject or the proper actions of the humanitarian organization. For example, the existence of public interest or a threat to the vital interests of an individual is too contextual a criterion to develop a standard practice applicable in any case. At the same time, it is the form of consent that raises the most questions. However, even if information is legally collected, what should be done with the data once it has been obtained?

Personal data storage. The main requirements for storing personal data are, first of all, ensuring their technical security – special (and limited) regime of access to servers, safe location of servers (avoiding states with a high index of human rights violations or directly personal data, occupied territories or territories with an uncertain legal regime), avoiding storing data on servers of companies that violate human rights and the like. In general, a transparency policy regarding how data is stored is also important in this matter: at the very least, a person can be warned in which country the servers are located and which legislation will be applicable in case of disputes.

Rights of the individual regarding his/her personal data. Apart from procedural issues, which depend to a greater extent on the activities of the humanitarian organizations collecting the data, the ICRC Handbook and other documents directly provide for the rights of data subjects. The key ones among these are the ability to correct outdated data, to have data amended or deleted at the request of the individual, and the right to object to the processing of data (or a particular type of processing). Let's look at what each of these rights means in practice.

- **Right to data rectification and change.** The person whose data is being processed has the right to request that the organization correct the information if incomplete, inaccurate

or outdated information about him or her has been entered into the database. This can also be done without proof of the correctness of the information in cases where the data is not important (typo, technical error, etc.). In cases where the data is important for determining the legal status of the person, it is possible to correct it by providing additional information (documents indicating age, details regarding gender, number of children, citizenship, etc.). Data correction occurs when an error has been made, whereas data change occurs when the data provided by the person was correct but has changed over time. For example, last name changed after marriage, the family was granted the status of a large family, etc.

- **Right to data erasure.** The Handbook stipulates several grounds for deleting data: the data is no longer needed for humanitarian aid, consent to data processing has been withdrawn, the data subject objects to the processing, or the processing no longer complies with technical and legal requirements for the personal data protection. The data subject may be denied the right to erasure if the processing is necessary to protect the interests of others, evidence of violations of humanitarian or human rights law, the basis of legal claims, etc., in short, if there is a legitimate interest in the further processing of such information. The grounds, however, may vary depending on the legislation of the country in which the humanitarian organization provides assistance or is registered.

- **Right to object to data processing.** Objection to data processing is a less radical form of opt-out compared to request for data erasure. In particular, it provides for the possibility for an organization to continue to store information without carrying out other types of data processing, such as analysis for statistics, data transfer, etc. However, as in the case of data erasure, it is possible for the humanitarian organization to continue data processing if there are legitimate grounds for doing so.

Data deletion due to limitation period. In general, the principles of data minimization and proportionality mentioned above explicitly state that using and storing data for longer than is necessary to fulfill the purpose for which it was collected will violate human rights. It is therefore an organization's main task to establish the point at which information is no longer necessary. The ICRC Handbook, in particular, contains a three-part test for this purpose:

- Assessment of the nature and sensitivity of the data;
- Assessment of the data storage format;
- Assessment of the amount of data and the type of their media.

The answers to these questions will allow you to find out how and when the data should be destroyed. In some cases, data can be anonymized or pseudonymized and then used for statistical or predictive purposes. For example, replacing full names with specific characters or other markers to the point where the data can no longer be matched to a specific individual. While humanitarian organizations should weigh whether this is proportionate to the cost of such activities, if information is stored on paper, it is unlikely that full anonymization will be possible, and digitization of data will require additional consent from the individual (unless obtained immediately for such data processing). Once data has been deleted or otherwise destroyed, the authorized person should ensure that the data cannot be recovered and that it has not been moved to other third-party media.

Data transfer to third parties. Data protection becomes a problem when data is transferred to third parties – the government, other organizations, subcontractors to perform certain tasks, etc. There may be many reasons behind this: for example, the organization can clarify data with local partners or share information with them in order to properly plan humanitarian actions, provide data to contractors for the production of supplies for people with special needs, share data when reporting to donor organizations. When any data transfer process takes place, it is important to

keep a few simple rules in mind:

- Organizations and individuals to whom personal data is transferred must ensure a similar level of technical and legal protection as those that collected the data and obtained the individual's consent to process and transfer it;

- The use of data by third parties for a purpose that does not correspond to the purpose of data collection violates the rules for handling personal data;

- Persons whose data is to be transferred to third parties should be warned about the transfer of information and its purpose. For example, the UN Office for the Coordination of Humanitarian Affairs has long had the problem that refugees were not properly explained the processes involved with their personal data, including the transfer of information to third parties (testimonies of refugees from Lebanon even became public in a retrospective assessment of this issue);

- The transfer of data to donor organizations should take place in anonymized or pseudonymized form, taking into account the potential risks of re-identification, data leaks, the reliability of donor data protection, the actual needs for obtaining such information and its use in accordance with the purpose of obtaining the data (which also implies the adherence to the principles of transparency and responsible data handling by the donor organizations themselves). Organizations that collect personal data should also warn that sensitive information may be shared with donor organizations for reporting purposes;

- Correlation of restrictions on data dissemination with the principle of system interoperability (if systems are interoperable, each requires less data in order to function fully, e.g. to identify a person). For example, the Eurodac system in the EU does not interoperate with the UN database in the Office for the Coordination of Humanitarian Affairs, which creates some inconvenience because both levels have to collect data from scratch. On the other hand, such a strict regime of data access and transfer protects information from reaching governments, because very often personal data is used to track individuals through various applications, track their whereabouts, occupation, etc.

- When transferring data across borders, the level of human rights protection in the state where the third party receiving the data operates should be considered. For example, data should not be transferred to authoritarian regimes, where data may be obtained by police or security services and subsequently used to target vulnerable individuals. Assessment should be made on a case-by-case basis, but organizations often use existing human rights protection rankings and indices developed by international organizations (e.g. Freedom House's Freedom Index).

Human rights impact assessment. Importantly, many international documents focus specifically on creating framework tests so that humanitarian aid organizations can self-certify that they are properly handling personal data or data that, in aggregate, could lead to the identification of an individual. For example, the above-mentioned Operational Guidelines on Data Responsibility in Humanitarian Action from the Interagency Standing Committee explicitly emphasize the need to assess the impact of data processing operations on data security and human rights. Moreover, such an assessment has several levels: It should be conducted both within organizations and in relation to external threats. The ICRC Handbook and the French regulator's Guidelines on personal data protection are framework documents on how to conduct a human rights impact assessment.

- **Internal control.** The internal control requirement is in line with GDPR standards regarding regular review of data handling policies and risk assessments for critical decisions. This

applies both to assessing strategic data handling plans and reviewing tactical decisions. For example, if there is a risk that an area where humanitarian aid has been provided will fall under occupation, whether it is advisable to continue storing data, whether it is worth destroying information contained on media in the risk area, etc. In internal assessment, an important role is played by so-called data protection commissioners, who should be in every organization and are responsible for complying with and putting into practice GDPR standards and other regulations, assessing risks and updating policies. In the context of armed conflicts, such a person should be aware of the requirements of international humanitarian law.

- **External audits.** Depending on the subject matter of the assessment, humanitarian organizations may also engage external auditors, provided they respect the principles of confidentiality and security. This may include civil society organizations and professional security auditors. Such auditing should take place in accordance with the standards that are partly outlined in the Handbook and Guidelines mentioned above.

The requirement to conduct risk assessments ultimately pushes for the creation of internal rules for handling personal data. Why is this relevant? Let us consider a few relatively new risks for humanitarian organizations. For example, an up-to-date risk roadmap has been developed by the human rights organization Privacy International.

Telecommunications. There is always a risk of interception of messages that may contain sensitive data, use of information to discredit a humanitarian organization, persecution of civilian, etc. It can also put the organization employees at risk, because in this way it is possible to track their movements and those of recipients of humanitarian aid. While these risks can be partially overcome through the use of secure communication services, many organizations and their staff still neglect the possibility of data leakage and surveillance.

Messengers and social media. The problem with over-reliance on social media and messengers is that they often use too much personal data, have access to other device functions, such as phone cameras or laptop data storage. In addition, the frequency and time of use of the services allows one to find out the approximate location of a person, daily routine, track contacts and movements using geolocation, etc. There is an even bigger problem with social media: Humanitarian organizations have no influence on their business model, data transfer to third parties, and protection against data leakage. Moreover, the use of platform services can contribute to additional monitoring of their activity by the state or illegal organizations (terrorists, extremists).

Smart cards. These are devices similar to electronic wallets, the tracking of which can reveal a person's location and movement, the amount of expenses and the timeline of the person's activities. Often humanitarian organizations are unable to provide aid directly and therefore use online transactions, which can create additional risks to the privacy of individuals.

Tracking technologies. The humanitarian sector and civil society organizations are often subject to surveillance by the state and illegal organizations. If humanitarian organizations are assisting vulnerable populations, they should be extremely cautious because various tracking applications and malware can get into working devices, databases, and technologies. In addition, using services from unsafe providers, unsecured communication networks and software that has not been vetted for compliance with human rights and privacy standards can pose additional risks of information leakage.

Technical malfunctions. The technologies that humanitarian organizations (or those with whom they collaborate to obtain data) use to collect and process information also play an important role in the protection and quality of the data collected. For example, when using facial or fingerprint recognition technologies, it is important that they correctly identify individuals and are also

interoperable. The discussion on this has continued in the context of the Eurodac system used in the EU. Thus, if there are multiple systems that identify individuals, if they are interoperable, each will collect significantly less data. If, on the other hand, they are not interoperable, each system will require significantly more information for each case of identification.

Cyber operations and cyber attacks. Many humanitarian organizations lack the expertise and technical defenses to detect and respond appropriately to cyber attacks against them. This often results in data leaks or the destruction of databases, as was the case with the databases of Save the Children, Human Rights Watch and other human rights defenders in 2020. Cyber operations by parties to armed conflict can also damage the infrastructure of organizations, preventing them from carrying out their humanitarian function. This is why there is a need to adapt technical standards to war contexts and develop crisis protocols that can be applied in emergency cases.

States that violate human rights. This is particularly relevant in the context of the establishment of occupation regimes by authoritarian states. For example, in Ukraine, Russian providers, Russian surveillance systems, a legal regime that allows law enforcement officials to have unlimited access to the servers of private companies and organizations and the like operate in the occupied territories. In addition, there is evidence that Russian police and administrations collect personal data of Ukrainians to allegedly distribute humanitarian aid or conduct censuses, although in fact they later use the information to persecute journalists, family members of military personnel, human rights defenders and activists. Even in cases involving democratic states, such as EU members, the question arises: Is the access of law enforcement agencies to most databases, such as information on migrants, asylum seekers, aid recipients, etc., proportionate? Often police and security services have access to more data than is objectively necessary for their work.

As a conclusion, there is a fairly extensive system of data protection standards by humanitarian aid organizations. The problem, however, lies in the status of such standards as soft law and the lack of a mechanism to punish for violations, especially given that many organizations operate across borders. However, regional regulations often fail to adequately address the realities of armed conflicts, while the emergence of new technologies and new challenges only complicates the tasks of humanitarian organizations to protect personal data. However, the general nature of the requirements of international law can be adapted at the national level, setting the necessary context and removing some risks through clarifications issued by national regulators. Therefore, in the context of Russia's armed aggression in Ukraine, the Ukrainian legislation should be considered in order to fully assess the landscape and security for the activity of humanitarian organizations in personal data protection issues.

SECTION III.
Data Protection Compositions – Ukrainian Style

According to UN statistics, a mere 71% of countries have legislation providing for the protection of personal data, while in other states the regulation is either at the stage of draft laws or does not exist at all. Humanitarian organizations operating or registered in Ukraine, in addition to international, rather framework standards, should be guided by national regulation. In the sphere of providing humanitarian aid, a special act will undoubtedly be the Law of Ukraine "On Humanitarian Aid", which defines both the requirements for the registration of aid and the conditions for its provision. However, before discussing such requirements, it is necessary to clarify how Ukrainian legislation understands humanitarian aid (in particular, during an armed conflict).

The Law allows the provision of humanitarian aid both to NGOs and charitable organizations included in the Unified Register of Humanitarian Aid Recipients and directly to individuals. At the same time, this Law does not regulate the issues of data protection of aid recipients in any way, not even referring to the relevant Law of Ukraine "On the Protection of Personal Data". On the one hand, this indicates that the legislator did not give much thought to data protection in emergency situations and did not develop special rules. On the other hand, it means that the general rules of the legislation on personal data protection are applicable in such circumstances.

Humanitarian aid is targeted free assistance in cash or in kind, in the form of irrevocable financial aid, voluntary donations, performance of work or provision of services from foreign or domestic donors to beneficiaries in Ukraine or abroad who need it due to social vulnerability, insecurity, difficult financial situation, emergence of a state of emergency or serious illness, as well as to prepare for the armed defense of the state and its defense in the event of an armed conflict.

So what does the Law of Ukraine "On the Protection of Personal Data" provide for and does it contain special rules applicable during a state of emergency or martial law? The object of regulation of this law is **personal data** itself – information or a set of information about a natural person who is identified or can be specifically identified. Identification in accordance with the Law of Ukraine "On the Unified State Demographic Register and Documents Confirming Ukrainian Citizenship, Identity or Special Status" provides for the possibility to clearly distinguish a person from others by means of any information, such as documents, biometric data or similar parameters.

The data that organizations collect for humanitarian aid is mainly for the purpose of identifying individuals in order to avoid the re-provision of one-off cash assistance, providing assistance for children to families that do not have them and the like. Although the amount and type of information collected depends on the type of aid (for example, full name, passport number or telephone number are almost always collected), personal data protection legislation will always apply to its processing. As a consequence, personal data can only be processed if one of the grounds set out in Article 11 of the Law is present.

Relevant **grounds for the processing** (collection, storage, transfer, etc.) of personal data in the context of the work of humanitarian organizations in providing assistance:

- Consent of the personal data subject to the processing of his/her personal data;
- Conclusion and performance of a transaction to which the personal data subject is a party or which is concluded in his/her favor;
- Protection of vital interests of the personal data subject.

Subject's consent. One of the most common grounds for processing personal data for the purpose of providing humanitarian aid is to obtain a person's consent. This is explained by the fact that the assistance is mainly provided by non-governmental organizations, and therefore the processing of personal data on the basis of the law cannot serve as a proper basis in such a case. Moreover, compared to other grounds, the subject's consent is easier to record and formalize.

> According to Article 2 of the Law, **consent** is a voluntary expression of will of a person (subject to his/her knowledge) to authorize the processing of his/her personal data in accordance with the stated purpose of their processing, expressed in a form that allows inferring the fact of consent granting. Online, consent during registration in the information and communication system (on the website) can be given by ticking the box with the permission to personal data processing (if the system does not process data before ticking the box).

Therefore, the Law establishes several requirements for consent: It must **be voluntary, clear, informed and obtained prior to the commencement of data processing** (except in cases like protecting the vital interests of the individual or other situations expressly provided for in Article 11 of the law). Such requirements for the form and nature of consent formally correspond to international standards for the protection of personal data during armed conflicts and the provision of humanitarian aid. However, in practice, problems arise with adequately informing beneficiaries about how much data is being collected, with whom it may be shared (for example, it is not specified that donor organizations will have access to the database), and the form of communication – overly legalistic language about where and how information is shared leads to misunderstandings about the implications of consent.

Finally, a major problem now is the virtual impossibility of refusing to provide personal data in such circumstances – in armed conflict, people are in desperate situations and often have no alternative sources of income, livelihoods or means of meeting domestic needs. As a consequence, providing consent is only a formality, whereas in practice individuals do not have the possibility to refuse. This should also be taken into account to prevent abuse by humanitarian organizations. Alternatively, in cases where an individual does not want his/her personal data to be stored by a humanitarian organization, instead of a humanitarian aid distribution sheet containing his/her personal data, the responsible official may draw up a report on the humanitarian aid received and distributed, which would be a proper basis for writing off the humanitarian aid from the organization's balance sheet.

Does the consent have to be in writing? The Law of Ukraine "On the Protection of Personal Data" does not limit the forms for expressing consent to the processing of personal data. However, the organization that provides humanitarian aid, in case of a dispute, will have to prove that the consent to the collection and processing of data was indeed given. Therefore, to avoid unnecessary disputes, it is worth recording the fact of giving consent. For example, some organizations use photo-fixation both to report on the proper distribution of aid and to protect themselves from possible lawsuits for illegal data collection. In this case, it is important to remember to ask for the person's consent to be recorded, as the mere act of posing (when a person is looking in the camera) is considered to be a form of consent.

At the same time, human rights activists note that in cases when a person calls to temporary help points or call centers, the question about first name and last name, phone number or e-mail address is not excessive, because the purpose is not to collect information, but to verify identity. Therefore, in such situations, it is not necessary to record a person's consent to data processing. At the same time, if data is collected over the phone to provide a particular service and that information is then stored or further processed, consent will be required.

The fact of consent to be photographed for the purpose of reporting to donor organizations and to confirm identity for humanitarian aid purposes **does not imply consent to the distribution** of such images to third parties or to the posting of photo/video in a public space (e.g. on social media to highlight the work of humanitarian organization). For such publications, the organization must obtain a separate consent of the person (Article 308 of the Civil Code of Ukraine).

At the same time, human rights activists note that in cases when a person calls to temporary help points or call centers, the question about first name and last name, phone number or e-mail address is not excessive, because the purpose is not to collect information, but to verify identity. Therefore, in such situations, it is not necessary to record a person's consent to data processing. At the same time, if data is collected over the phone to provide a particular service and that information is then stored or further processed, consent will be required.

Conclusion and performance of the transaction. As explained by the Human Rights Platform experts, referring to the norms of the Civil Code of Ukraine, when concluding any contract, a person is obliged to identify himself/herself. Thus, Article 28 indicates that a person acquires rights and obligations and exercises them under his/her own name, and Articles 202 and 626 respectively indicate that the transaction provides for the acquisition, modification or termination of rights and obligations, including through the conclusion of a contract. Since the conclusion of a contract on the provision of charitable assistance itself provides for the consent of the person to the terms of the contract, additional consent under Article 11 of the Law of Ukraine "On the Protection of Personal Data" is no longer required. At the same time, part 2 of Article 12 of this Law provides for notification of the person about what data is collected and for what purposes it is carried out. Therefore, the contract must clearly specify the amount of information that is collected and the purpose of its processing. If this is not done, the individual will have the right to appeal, for example, against the fact that the organization collects an excessive amount of data or uses the information already collected for purposes other than the intended purpose (e.g. for marketing purposes, etc.).

Protection of the vital interests of the individual. This ground is most often used when it is necessary to provide emergency medical care, rescue a person from unlawful attacks or carry out rescue operations. However, in the case of a humanitarian disaster in a certain region, it can be assumed that humanitarian organizations may process data before obtaining the consent of the individual. For example, there is no physical possibility or sufficient time for explanations, which nullifies the validity of consent (because it should be based on prior full information), the person is in a bad psychological and emotional state, which makes clarification impossible, and so on. In their explanations, the Ombudsman also notes that this ground is applicable in cases where the person is generally unconscious. However, the basic rule of this ground for the processing of personal data is to obtain the consent of the person to the processing of the data as soon as it becomes possible.

If, after the opportunity arises, the individual's consent has not been obtained or the individual expressly objects to the processing of personal data, the organization is obliged to **stop such processing and delete the already obtained information.**

In case of termination of data processing due to failure to obtain consent, of course, the issue of reporting by humanitarian aid organizations to international donors and state authorities, if they cooperate, is relevant. However, in such a case, the humanitarian organization may provide anonymized data about the person: street of residence without a specific address (in cases where the person's origin is key), gender, social status (person with disability, work specialty, etc.), age range, etc

In addition, experts note that the use of personal data may involve various actions related to their collection, distribution or storage, however, the key is the compliance of such actions with the purpose of data processing. An obvious example: if the data is collected for the sole purpose of humanitarian aid, its use for marketing purposes would be contrary to the requirements of the law. Where possible, human rights defenders emphasize that information about a person can be obtained from official documents issued in the person's name and public records. However, the processing of information from public sources still includes an obligation to notify the individual that his or her personal data is being used to provide certain services, such as humanitarian aid.

> **Important!** When collecting personal data for the provision of humanitarian aid, organizations must adhere to the **principle of data minimization**. For example, disproportionately large amounts of personal information should not be collected; information about sexual orientation, gender or ethnic origin is often unnecessary. Information on age or marital status may also be unnecessary if it is not relevant to the type of assistance being provided.

Storage of beneficiaries' personal data. In addition to the existence of grounds for data processing, the data owner (i.e. a humanitarian organization) is obliged to create a database of persons receiving humanitarian aid, develop internal rules for data processing, provisions on such a database (which will be accessible to aid recipients, human rights defenders, journalists, etc.) and appoint the person responsible for the data processing and their protection. This is due to the fact that data controllers and owners are more aware of what data should be processed and how, as well as their technical capacity to ensure the protection of servers, their location and the transfer of data between databases in case the owner or controller has several of them. Some specifics of the regulation are provided for by the Standard Procedure for Processing Personal Data approved by the Order of the Human Rights Commissioner of the Verkhovna Rada of Ukraine No. 1/02-14 back in 2014. This Standard Procedure determines, among other things, certain organizational obligations of owners and controllers:

- Determination of the procedure for access to personal data by the organization employees;
- Determination of the procedures for recording transactions involving the processing of personal data;
- Development of a plan of action in case of unauthorized access to the data storage, damage to technical systems or other emergencies (in the context of armed conflict, the possibility of occupation of the territory, etc. is relevant);
- Training on personal data protection for employees

In accordance with the Standard Procedure, personal data must be processed and stored in such a way as to prevent access by third parties, which is especially relevant when it comes to automated data processing that can be accessed via the Internet. Given that automated systems may have technical faults, the need for regular technical inspections of such systems should also be taken into account.

Dissemination of beneficiaries' personal data. As mentioned above, the personal data collected in the process of humanitarian assistance should often be used by organizations for reporting to international donor organizations, government agencies, etc. The data may also be stored on foreign servers, where their technical security is ensured by third-party companies. Personal information can be used to build logistics and predict future needs, which is sometimes done by organizations other than those directly providing humanitarian assistance. However, it should be remembered that any dissemination of personal data to third parties must be communicated

to humanitarian organizations in advance, having obtained the consent of the data subject. Moreover, such data transfer must be consistent with the purpose of data collection: for example, obtaining consent to data transfer to other organizations for humanitarian aid, when in fact the organization will be transferring the data for marketing or research purposes, would be a violation of the right to protection of personal data.

> The third party to whom personal data is to be transferred must ensure that all standards of such data protection are met, both technically and legally. The obligation to verify whether the third party is able to comply with the standards **rests with the data owner** who plans to transfer the data, in this case the humanitarian organization.

Needless to say, failure to ensure technical or legal protection of personal data implies that the data cannot be disseminated to such a person, company or organization. In general, the rule on the development of internal regulations also applies to third parties, which, in particular, will regulate the access of employees to databases and servers, define the conditions for data deletion or rectification, etc. At the same time, protection must be ensured not only by the organization or person to whom the data is transferred, but also in the process of information transfer. A relevant question arises: what should we do when a humanitarian organization operates in the occupied territory or the territory adjacent to the occupied territory, in the so-called gray zone?

How to process personal data during martial law? Despite widespread expectations, trends on the part of the state do not indicate an increase in the number of restrictions, but rather an improvement in the protection of personal data. As the war in Ukraine is characterized by the constant change in the front line and the changing status of territories (occupied, de-occupied, frontline and border zones), secure data storage is an important issue. Since March 12, 2022, the Resolution of the Cabinet of Ministers of Ukraine "Certain Issues of Ensuring the Functioning of Information and Communication Systems, Electronic Communication Systems, Public Electronic Registries under Martial Law" has been in force, which prohibits the use of cloud resources and data processing centers located in the temporarily occupied territories of Ukraine. Experts generally support such a restriction, because it allows avoiding situations of seizure of databases and their use by the occupants to persecute journalists, activists, human rights defenders and other vulnerable groups who participate in the provision of humanitarian aid or receive it. The ban also applies to cloud resources and storages that are located on the territory of the aggressor state, belong to entities registered in it (for example, data storage in Germany founded by a Russian company) or states that are members of customs or military alliances with the aggressor state. Thus, the restrictions apply not only to Russia, but also to Belarus and a number of other post-Soviet countries.

Initiatives that indirectly affect the protection of personal data in the humanitarian sphere. This mainly concerns the access of state authorities to databases, including those owned or managed by private organizations (Ukrainian and foreign). Among the most influential initiatives, it is worth highlighting the amendments to the Criminal Procedure Code of Ukraine

- **Law No. 2111** of March 3, 2022, which concerns the facilitation of investigative actions during martial law;
- **Law No. 2137** of March 15, 2022, which covers changes to the procedures for inspection of the scene, searches, temporary access to computer systems and data, the possibility of copying recordings from surveillance devices, which also applies to cases of suspected fraud by humanitarian organizations (where, as a result of the initiation of proceedings, investigators will have unlimited access to databases of vulnerable groups).

In addition to the simplification of the investigative procedures themselves, the process of coordinating investigative actions has also been "eased": While previously it was necessary to obtain a ruling of the investigating judge, now it is enough to apply to the head of the prosecutor's office in cases where the investigating judge is objectively unable to provide such authorization. That is, at least in this case, when obtaining authorization, it is necessary to conduct a contextual assessment of the circumstances in which the investigation is taking place.

The situation changed in July 2022, when amendments were introduced to Article 615 of the Criminal Procedure Code of Ukraine, which dealt specifically with the issue of access to personal data. According to the new rules introduced for the duration of martial law, the prosecutor may authorize temporary access to information that is stored by the person or in the personal data base of the data owner. As lawyers point out, unlike other investigative procedures, these changes do not depend on the availability of the investigating judge and simply make it possible to access information on private servers only on the basis of the prosecutor's decision (this decision is then coordinated with the head of the prosecutor's office). That is, there is a risk of disproportionate interference in cloud storage and databases owned by humanitarian organizations.

As a result, threats to personal data generally exist in different contexts: ranging from external threats in the form of hacking attacks, data leaks and the use of databases to target vulnerable groups, to potential excessive state interference in such databases created by humanitarian organizations. As there is currently no specific regulation on the processing of personal data specifically during armed conflict and in the context of humanitarian assistance, organizations are guided by general data protection standards.

Although there have already been several attempts to update the legislation on personal data protection and harmonize it with European standards and GDPR, one draft law was rejected by the Parliament, while another is still under consideration in the relevant committee. This means that the collection, storage and dissemination of personal data must now comply with the grounds for data processing, as well as the principles described in the previous two sections – international standards and current national regulation. Are these standards applied in practice in the work of Ukrainian and foreign humanitarian organizations? This can be found out by analyzing their data protection policies and the media context for situations of personal data breaches.

SECTION IV.
Are Humanitarian Organizations in Tune With the Standards?

Personal data protection standards – both national and international – are more or less generic. This makes sense, as they are aimed at a huge number of organizations of different sizes and ways of working, which apply different means to process information and operate in different contexts. As a consequence, the key question is not only whether standards are embedded in companies' corporate policies, but also whether they are well incorporated and whether they can be effectively applied in practice. Therefore, the aim of the research was to establish what companies are guided by when collecting and processing data and to find out whether such policies comply with the standards and whether it is possible to improve personal data practices.

For ease of analysis, four main categories of organizations performing humanitarian functions were identified. The categorization depended on the specifics of their legal regulation (in particular, jurisdictional issues), the way they are formed and administered, the way they provide humanitarian assistance, and the scale of their work. Thus, the study assesses the policies and practices of intergovernmental organizations, international, foreign and national humanitarian organizations.

Intergovernmental organizations

This category includes those providers of humanitarian aid which are often referred to simply as international organizations in the media — various bodies within the UN structure (UNESCO, UNICEF, UNHCR, etc.), the Directorate General for European Civil Protection and Humanitarian Aid Operations, etc. All these organizations have a special procedure for the development, approval of humanitarian aid programs and special rules for handling personal data. Depending on the type of assistance, the amount of data collected, the procedure for its storage and processing, and the way it is collected differ.

At the same time, status and official status do not protect from problems related to data leakage or cyberattacks. For example, in 2019, there was an attack on the UN database at the UN headquarters in Geneva, which resulted not only in a data breach, but also undermined confidence in the institutional capacity of an organization like the UN to protect data. That is, not only the personal data itself is at risk, but also the reputation of the key institutions and their ability to further ensure the provision of humanitarian assistance. So let's find out whether the key international actors have sound policies and are putting them into practice.

UN Refugee Agency (hereinafter UNHCR). This organization was the first UN structure to develop and successfully implement separate policies on personal data protection. Interestingly, this happened only in 2015. Before that, the organization, like all other parts of the UN, was guided by general international standards and national requirements. Now there is a separate document – the Policy on the Protection of Personal Data of Persons of Concern to the Agency.

In 2018, Alexander Beck, Senior Data Protection Officer at the UNHCR, noted that the development of a separate protection policy was motivated by the fact that key international documents are unable to adequately address new threats to data generated by the development of automated data processing technologies, new cyber threats, social media, etc. So what does the policy itself look like? Let's take a look at its main provisions and see if they properly address personal data protection risks.

The Personal Data Protection Policy explains in some detail UNHCR's approaches to data protection and its transfer to third parties:

- **Data protection principles** (existence of legitimate grounds and clarification of the purpose of data processing, data accuracy, respect for the principles of necessity and proportionality, confidentiality and data security, respect for the rights of others and accountability for breaches);
- **Rights of the personal data subject** (access to information; rectification and erasure of data, objections to data processing, restrictions that make it possible to process the data subject's data even in the presence of objections on his/her part);
- **Data processing conditions** (data confidentiality and security; technical requirements for passwords, data access, data transfer procedures within the organization; notifications of data protection breaches);
- **Requirements for compliance with the policy by partner organizations** (including termination of partnership relations in case of data protection breach);
- **Transfer of data to third parties** (priority of maintaining trust in UNHCR and effective humanitarian assistance, special rules on data transfer agreements with third parties, special rules on transfer of data to law enforcement agencies, data protection for persons with immunities);
- **Existence of a data protection officer** (monitoring of policy compliance, providing advice on the implementation of new practices of personal data handling, keeping documentation on data collection and processing, reporting on the effectiveness of data protection policies).

Although, in general, the almost 50-page document details the rules of work with personal data quite substantially compared to general international regulations, the question of what technologies are used is still relevant. Thus, the policy does not set any restrictions on working with systems controlled by artificial intelligence, facial recognition technologies, does not address dangers from social media and the like. In fact, the document does not establish strict rules for handling biometric or other sensitive types of data. As a consequence, while the policy is quite detailed, it all comes down to its application in different contexts.

Are policies effective in practice? In 2019, Dragana Kaurin prepared a study on international organizations' privacy policies and their application to real-life scenarios. The UNHCR was the key focus of this study. Its results do not look very comforting, at least according to the feedback from those who received humanitarian aid and registered as refugees.

Thus, organizations that provided humanitarian aid and assisted in the registration of persons as refugees often requested excessive amounts of data: for example, they recorded information about sexual orientation, education or ethnicity, the presence of incurable diseases (such as cancer or AIDS). Biometric data such as fingerprints, retina prints or ordinary face photos were also often collected. One of the most common justifications is that it helps prevent fraud and provision of aid to the same person twice. At the same time, research shows that both fingerprints, and facial recognition can be inaccurate, because the systems often reflect institutional discrimination. Moreover, when assisting refugees from Myanmar in 2018, UNHCR created profiles on the people it assisted. One of the criteria was ethnicity, which created risks of repatriation of the ethnic Rohingya community due to the discriminatory authorities of Bangladesh, where Myanmar nationals fled the genocide. In addition, while assisting Syrian refugees in Lebanon in 2014, UNHCR faced the problem of the Lebanese government demanding access to the refugee

database. That is, collecting excessive amounts of data is not only disproportionate, but often dangerous for the recipients of humanitarian aid, as neighboring governments can be quite hostile.

In addition, beyond simple data collection, verification of information is often a challenge. In particular, if assistance was primarily intended for survivors of sexual or physical violence, torture or inhuman treatment, for pregnant women or persons with chronic illnesses, organizations required verification of this status. Because refugees often lacked health records or proof that they had suffered from crimes, the procedure itself was very traumatic for such individuals. For example, Kaurin recalls a case where 6,500 refugees in Mauritania were denied access to food, medical care and other essential services because the system misidentified them.

Finally, although UNHCR's policy contains a very detailed explanation of the purpose of using the data, refugees note that in practice, aid providers did not explain anything. That is, the policy is often declarative. For example, Syrian refugees in Greece could not get proper explanations as to the reasons for fingerprinting, while the only response was that it was a "normal procedure". As a consequence, policy language alone is apparently insufficient to effectively protect the personal data of humanitarian aid recipients.

Although no such cases have been identified in Ukraine, mainly due to the more tolerant attitude of Europeans towards refugees and better coordination of humanitarian aid processes, excessive data collection still happens, because biometric identification is part of the general mechanism for establishing the identity of the beneficiary. That is, in case of data leakage, UNHCR risks facing problems with the use of collected data by malicious actors, including those from an aggressor state.

UNICEF. The organization works a lot "in the field", it is directly involved in humanitarian missions, operates large amounts of personal data, and therefore needs detailed data protection policies. For example, in Ukraine, UNICEF provides monetary assistance under the Spilno project, which involves obtaining a basic set of personal data to identify individuals and their social status.

UNICEF has a separate Personal Data Protection Policy 2020, a fairly brief document outlining the basic principles of handling such information. Important elements of the policy:

- **Principles** (legitimate grounds for data processing, compliance with the purpose of data processing, data sufficiency and quality, necessity and proportionality, security, limited data storage period);
- **Notification of data processing;**
- **Rights of the data subject** (access to information, right to rectify data, object to processing, request erasure, right to object to automated decision-making);
- **Transfer of data to third parties** (without any details);
- **Liability and extraordinary measures** (in contexts where it is not possible to enforce the policies as presented and a procedure for derogations);
- **Supervision of compliance with data protection policies** (with detailed procedures);
- **The best interests of the child** (UNICEF notes that the processing of personal data must not violate the interests of the child in any case).

Among the points of obvious concern, it is worth noting that among the "legitimate interests and grounds" for data processing, UNICEF notes "other interests", a category that can be interpreted very broadly. On the other hand, the data storage period is limited to 10 years, and if this period is exceeded, UNICEF must further justify the need for further data storage.

Finally, UNICEF has developed expanded Guidelines on Privacy, Ethics and Data Protection that detail all procedures and processes to be followed when providing humanitarian assistance.

As can be seen, the policy is rather general and rather framework-like, which implies many practical challenges in its application, in particular, in the issues of assessing voluntariness and informed consent, automated data processing, etc. Data collection is often problematic when the explanation of the data collection purpose (in the amounts collected) and the fate of the information collected are not clear.

In addition, in Ukraine, UNICEF even became involved in a scandal around the organization's disregard for the provisions of Ukrainian legislation on data protection. This, in turn, made many people wary of receiving assistance in international centers. For example, last year there was a scandal about the unlawful collection of personal data by UNICEF as part of the financial aid program "Spilno", which is designed to allocate funds to large families or families with children with disabilities. It made sense in this case to collect information about the number of children in the family and their state of health. At the same time, blogger Serhii Hula noted in his video that UNICEF does not obtain permission to process personal data, uncontrollably transfers it to third parties and does not implement any security safeguards, violating the Law of Ukraine "On the Protection of Personal Data".

As it turned out, there were no violations on the part of UNICEF. Ukrainian fact-checkers from VoxCheck told about it in their research. In particular, they checked the rules of personal data processing, which UNICEF follows, as well as the identity of the lawyer who disseminated information about the illegal collection of personal data. It turned out that it had made false statements in the context of the pandemic and vaccination before, so the misinformation spread was not the first episode. However, such actions are quite dangerous, as they undermine trust in international institutions and make people who need help afraid to seek it for fear of fraud and rights violations.

However, this does not mean that there were no violations on the part of UNICEF at all. In 2019, for example, a glitch in an online training course system exposed the personal data of some 8,200 users. The data leak involved the dissemination of names, email addresses, age, gender, organization, and even the types of contracts an individual had. On the positive side, UNICEF was quick to acknowledge the problem and even explained that the data leak was caused by a technical error made by a staff member.

As you can see, even the UN institutions are not perfect when it comes to data protection, and here a lot depends on the human factor. At the same time, one should be very cautious about information available online regarding violations of the rules for handling personal data. Otherwise, misinformation may undermining the reputation of humanitarian organizations and lead to the failure to provide assistance to people who really need it.

European Council for Refugees and Exiles. It is worth considering a regional institution to compare with the policies of organizations within the UN structure. The European Council appears to be the closest to the Ukrainian context and therefore the most relevant humanitarian aid agency. This organization, like many others, has developed separate data protection policies adapted to humanitarian contexts.

The European Council's rules on personal data are called "Data Protection: Privacy Policies and Guidelines" and are quite concise and clear:

- **Principles** (data minimization, legitimate grounds for data processing);
- **Dissemination of information to third parties** (in particular, disclosure of which third parties have ongoing technical contracts with, e.g. Google, Microsoft, etc.);
- A separate **person responsible for data protection;**
- **Registration of activities** involving data processing;
- **Breach notifications;**
- **Primacy of the GDPR** over other regulations and constant references to its provisions.

It is indicative that, unlike the UN institutions, the European Council has an exhaustive and clear list of grounds for data collection and processing, and the category of "public interest" is disclosed and accompanied by the European Council's obligation to balance interests and ensure compliance with the principle of necessity and proportionality. At the same time, public policy lacks information on what rights subjects have and how they should approach the organization to exercise such rights.

It is also important that the European Council acts as one of the EU institutions. Accordingly, it is subject to personal data protection requirements, including in the policies of websites that EU bodies create. In practice, this means that websites must include a cookie warning and similar information about the data they collect on an individual before they even consider providing aid or other humanitarian action. At the same time, the European Council has not been featured in any scandalous stories about data protection breaches, which gives hope that the legal and technical protection of information obtained in the course of humanitarian aid is sufficiently strong.

In addition to the organizations analyzed, whose work is most relevant in the context of Russia's armed aggression in Ukraine, there are other humanitarian organizations, such as the UN World Food Program (which has policies as much as 130 pages long), the UN Office for the Coordination of Humanitarian Affairs, the International Organization for Migration, the European Commission's Directorate General for Civil Protection and Humanitarian Aid and many other specialized bodies. Most of them have data protection policies, the level of detail of which varies depending on the age of the document and the contexts the organizations have encountered in their work, but a common challenge is the application of written principles and rules in practice.

International non-governmental organizations

International non-governmental organizations, unlike governmental organizations, are freer in what means to use to collect personal data for humanitarian assistance. Moreover, they are also more flexible in reporting and oversight processes, as well as in the establishment of bodies that deal with the provision of assistance. On the other hand, non-governmental organizations often face the issue of reporting to donor organizations for the humanitarian assistance provided. Thus, they have to report the number of persons who have received it, the fulfillment of formal requirements for assistance (for example, the fact that the family has many children or that the person has health problems, etc.). This in turn gives rise to a new category of problems.

It would seem that international organizations that deal with such sensitive issues and whose offices are located in democratic countries are able to provide one of the highest levels of protection for the data collected. In practice, however, things are not so simple. For example, in

January 2022, on the eve of Russia's full-scale invasion of Ukraine, there was a massive leak of data from the ICRC's database (data on some 515,000 people), leading to disruptions in humanitarian operations. And this is just one example of how vulnerable non-governmental organizations are. Overall, statistics show that about two-thirds of non-governmental organizations have been the target of hacker attacks or data breaches at various times, and do not pay adequate attention to cybersecurity risk assessments. In other words, there are many challenges facing global international non-governmental organizations right now. The only question is whether they are able to deal with these challenges in a way that does not put their beneficiaries at greater risk.

ICRC and the International Federation of Red Cross and Red Crescent Societies (hereinafter referred to as ICRC and IFRC). Contrary to popular belief, the ICRC and the IFRC are not the same organization. They have slightly different mandates, decision-making procedures and, importantly within the scope of our topic, different personal data protection policies. However, since these two institutions are quite closely related, they should still be evaluated by comparison to understand the extent to which policies can be inconsistent with each other even in "sister" organizations.

ICRC Personal Data Protection Rules	IFRC Personal Data Protection Rules
The scope and detail of the provisions in the rules resemble the structure of UN documents, so they are quite comprehensive: ■ **Principles** (legitimate grounds for data processing, transparency, compliance with the purpose of data processing, data sufficiency and quality, archiving or deletion of data that are no longer relevant); ■ **Rights of the data subject** (access to information, right to rectify data, object to processing, request erasure, right not to receive decisions based on profiling); ■ **Possibility to derogate from duties in emergency situations;** ■ **Data protection model by design and by default;** ■ **Personal data impact assessment** (the organization should assess data handling policies contextually and as quickly as possible); ■ **Documentation of data processing;** ■ **Cooperation with supervisory authorities** (national or regional level); ■ **Breach notification and liability;** ■ **Transfer of data to third parties** (including law enforcement authorities and access for genealogical and administrative research); ■ **Data protection office and commission** (as supervisory bodies of the ICRC, which decide on personal data practices and handle breaches respectively).	The policy itself is quite short and concise, but generic in nature. Particularly, it contains several sections specifying the rules of data processing: ■ **Principles** (existence of legitimate grounds for data processing, access to information, clarification of the purpose of processing, data minimization, data storage for no longer than necessary, data security and confidentiality); ■ **Rights of the data subject** (access to information, right to rectify data, object to processing, request erasure, receive a timely and understandable response to requests); ■ **Assessment of the impact on personal data** (the organization must evaluate new technologies, review automated system solutions, assess contextual risks in the context of the application of mass surveillance); ■ **Breach notification and liability;** ■ **Transfer of data to third parties** (including law enforcement agencies).

ICRC Personal Data Protection Rules	IFRC Personal Data Protection Rules
However, in the wording of the Rules, there are grounds for data processing such as «the pursuit of the legitimate goals of the ICRC, as long as this does not harm the rights of the subject» and «compliance with legal requirements / obligations», which can provide for virtually any ground available in the ICRC's statutes, its contracts with other entities or other internal documents. In addition, if the ICRC operates in authoritarian countries, a dilemma may arise: provide personal data to authoritarian governments or disobey local laws. Currently, the Rules provide for compliance with the law without any exceptions or reservations, which may lead to human rights violations. Also, one of the purposes of data processing is to «build respect for humanitarian law», which raises quite a few questions in the context of personal data (in particular, anonymized and pseudonymized data can be used for trainings and roundtables). Finally, instead of deleting data, the Rules provide for archiving in cases where it is useful for statistical, historical or scientific purposes, i.e. in virtually any situation. This in turn poses certain risks, as digital archives can still be subject to hacker attacks. At the same time, the ICRC has a shortened and simplified version of the Rules on its own website, which explains in detail the rights of subjects and allows them to understand what happens to the personal data collected and how to make a data request to the ICRC. This is certainly a positive step, as it facilitates clarification and is also in line with the principle of transparency.	Of concern in the Policy wording is the presence of grounds for data processing such as «pursuit of legitimate Federation purposes» and «performance of tasks in the public interest», which could provide for virtually any ground available in the IFRC's statutes, the Federation's contracts with other entities, or other internal documents. This can become dangerous, especially when the organization is not fully aware of the context of the work and, for example, is collaborating with a government that may resort to human rights abuses. There is also a lack of details on an individual's consent, the conditions for recognizing it as valid, the conditions for automatic deletion of information when the data retention period expires, etc. At the same time, the organization has several separate guidance documents for dealing with data or funds transfer systems. For example, the Practical Guidance on Data Protection when providing assistance in cash and voucher form provides more detailed rules for the provision of assistance based on the format and available means of providing such assistance.

As with UN institutions and other international organizations, the ICRC and the IFRC have general policies that depend significantly on practical application. So the key question is: are these humanitarian organizations as conscientious in practice as in written policies?

This is questionable, to say the least, as the ICRC is quite active in collecting biometric data from recipients of humanitarian and other forms of assistance. For example, the organization uses software on the Trace the Face website to recognize the faces of refugees, asylum-seekers and recipients of humanitarian assistance in order to restore family ties. The website itself does not provide any information on how personal data is processed and stored, either legally or technically. Furthermore, the website stores images that are more than 10 years old, so it is not

known whether facial recognition technology is also applied to them, and if so, whether this was authorized at the time the data was collected.

The case of the hacker attack on the ICRC database, during which some 515,000 people were left really vulnerable, has already been mentioned. From a technical point of view, this pointed to gaps in the protection system and also to the impossibility of fully securing data against hacker attacks and external threats. On the positive side, at least the ICRC reported the data leak in a timely manner, reporting the amount of information lost and those affected. The committee even released details of the attack and its aftermath. At the same time, after the incident, the Ukrainian Parliament Commissioner for Human Rights asked the ICRC to report on data protection procedures.

International Rescue Committee (hereinafter referred to as IRC). Not all organizations have detailed data protection policies. In some cases, they are even hard to find with a free Google search. And the IRC is one of them.

IRC data protection policies vary by region: The organization's website gives you the option to choose from several options (US, UK, Germany, Sweden, EU and Korea). In this analysis, we focus on a policy that is considered global, the Privacy Policy. Unlike the policies of many other organizations, this document is posted in a separate section of the website, and therefore may be updated regularly (readers may not notice this). However, the structure of the document is quite clear:

- **A list of the data collected** (in particular, cookies, data required for cooperation with IRC, and information provided to subscribe to updates);
- **Transfer of data to third parties** (providers, charitable organizations, within legal proceedings, in exceptional cases – transfer of data for business purposes);
- **Data protection** (technical protocols);
- **Cookies** (detailing the purpose, method of collection and explaining the technical side of the process of setting cookies on the website)
- **Reference to GDPR;**
- **Children's privacy** (specific rules).

In addition to the website use policy, there is also an Organizational Policy. It is more applicable to the humanitarian aid process. However, it does not contain any details on data protection, the rights of subjects or the possibility of data deletion:

- **References to the GDPR** and the general duty of respect for privacy;
- **Non-exhaustive list of data** to be collected;
- **Ban on the free dissemination of refugee biometric data** without the consent of the U.S. Bureau of Population, Refugees, and Migrants.

Notably absent from the Policy, which deals specifically with "work in the field", are any details on the rights and abilities of subjects to send requests for data erasure or correction, object to data processing, and the like. There are also no general principles that guide the organization's handling of data. This is a rather dangerous trend, especially since the organization positions itself as a leader in humanitarian aid. At the same time, a positive aspect of the policy is its illustrative nature: model situations are given to demonstrate how the IRC will respond to certain requests from the public.

On the positive side, IRC uses a Box Shield system that provides enhanced protection of personal data through an additional authentication system. In general, this is a positive step, because it allows preventing data leaks. On the other hand, the use of a third-party system indicates that IRC does not have its own developments in this field, that is, it uses external resources.

Save the Children (hereinafter referred to as SCI). The organization is highly specialized and works directly with vulnerable groups and sensitive information. Accordingly, this contributes to the creation of a special procedure for handling personal data.

Data Protection Policy is a small structured file that sets out the basic principles for handling personal data, with a focus on the sensitivity of data relating to children (in particular **the best interests of the child):**

- **Reference to the GDPR** (including the existence of a data protection officer);
- **Principles** (legitimate grounds for data processing, transparency, compliance with the purpose of data processing, data minimization, data quality, archiving or deleting data that is no longer relevant, confidentiality and accountability);
- **Staff training on data protection** (every 12 months);
- **Consent to data processing** (active, conscious and informed consent, availability of parental consent for children (persons under 18 years of age);
- **Transparency and information** (quantity of data, purpose of collection, legal basis, duration of data storage, transfer of data to third parties);
- **Assessment of impact on personal data** (privacy by default, the organization must evaluate new technologies, especially regarding the collection and processing of sensitive data);
- **Rights of the data subject** (access to information, right to rectify data, object to processing, request erasure, receive a timely and understandable response to requests, right to be forgotten);
- **Transfer of data to third parties** (including international data transfers);
- Data security (administrative and technical measures);
- **Breach notification and liability.**

Of concern in the Policy wording is the presence of grounds for data processing such as "pursuit of legitimate SCI purposes" and "compliance with legal requirements / obligations", which could provide for virtually any ground available in the articles of association, contracts with other entities, or other internal documents. This can become dangerous, especially when the organization is not fully aware of the context of the work and, for example, is collaborating with a government that may resort to human rights abuses.

At the same time, SCI has separate guidelines on how to obtain consent for data processing, breach reporting, cybersecurity and other procedural aspects. An abbreviated version of the privacy policies is set out in accessible form on the organization's website, with links to basic subject rights, data categories, and activities for which data is collected. The organization also has separate websites and separate policies for regional offices, such as the USA.

However, well-designed policies do not mean that an organization has never been the target of attacks or has a perfect data protection history. In 2018, for example, fraudsters posing as an employee forged invoices and stole about $1,000,000 from the organization's accounts. In a similar scheme, fraudsters could also gain access to personal data. Another case was security gaps. In July 2020, there was a cyberattack on one of SCI's software vendors, which

the organization reported on its website. Unfortunately, the data breach also affected SCI's beneficiaries, including age, gender and history of children's involvement in the organization's programs. This demonstrates the organization's relative inability to predict cyber challenges, especially when it relies on third parties for data storage on servers, etc.

In addition to the companies analyzed in detail, we also considered and interviewed NGOs such as Medicos del Mundo, HelpAge International, Triangle Génération Humanitaire, Premiere Urgence Internationale, Handicap International and Red Rose CSP. By general standards, most policies are quite similar among humanitarian aid organizations. The difference is noticeable mainly in issues that relate to their work focuses: vulnerable minorities, persons with disabilities, children, etc. As a consequence, the prevalence of a sensitive category of data may make organizations' privacy policies tailored to address specific problems. However, in practice, security problems and relative technical insecurity are quite common.

Research shows that NGOs often lack the technical expertise, human, financial, and/or technical resources to adequately anticipate and prevent technical threats (such as data breaches, hacking attacks, or employee negligence). As a result, non-governmental organizations are characterized by a reactive rather than a proactive approach to countering cyber threats. This in turn is very dangerous in the humanitarian context, because in the case of database hacks, information leaks or technical malfunctions, it is virtually impossible to restore the previous state of affairs – personal data will already be in the hands of criminals. Therefore, humanitarian organizations should pay special attention to preventing threats in advance rather than reacting to them after they occur.

Foreign local organizations

Local organizations with cross-border projects (humanitarian aid abroad) have their own peculiarities in dealing with personal data. They must create policies in accordance with the laws of the state in which they are registered and the state where they provide assistance. While in theory this is simple, in practice the legislation is too general and it all depends on how internal policies are worded, where the data is stored and with whom it may be shared as a result. Given the fact that public attention to such organizations is less meticulous compared to ICRC or other humanitarian "giants", the question arises: are organizations just as conscientious about adhering to data regulations? For example, in Italy, humanitarian organizations collected data on a refugee's sexual orientation when providing aid. The purpose of such data collection was not disclosed, which caused even more discomfort for a person already in difficult circumstances (not to mention the principle of data minimization).

People in Need (hereinafter referred to as PIN) (Czech Republic). This is a Czech organization that provides assistance and legal support in many regions, including Ukraine. PIN belongs to organizations that work "in the field", that is, collect personal data during the provision of assistance. In addition, PIN is one of the few organizations that responded to the UMDPL survey by explaining how they store and protect personal data, what documents they follow and what standards they apply. Of importance, PIN cited two documents on which their policies are based, the ICRC Handbook on Data Protection during Humanitarian Action and GDPR. In response to UMDPL's request for clarification of data protection practices, PIN noted:

> ***"The basic principle of all PIN's data protection policies is that our activities, if they involve handling the personal data of PIN beneficiaries, are carried out with professional care, in a transparent manner and in a way that respects the rights of the individual in terms of protecting their personal data. The requirements of all internal guidelines shall be applied to the fullest extent possible also in cases of cooperation with other entities (organizations that come into contact with any personal data of PIN or PIN beneficiaries on the basis of a contractual relationship)."***

ЦThis means that similar policies apply to third parties that cooperate with PIN to provide humanitarian assistance: its local partners or vice versa — umbrella organizations at the international level. This is also positive in the context of assistance in Ukraine, which involves cooperation with local organizations.

The Data Protection Policy is available online and covers very general information handling rules. In particular, it contains:

- **Reference to the GDPR** (including the existence of a data protection officer);
- **Principles (**legitimate grounds for data processing, compliance with the purpose of data processing, necessity and proportionality);
- **Types of data most commonly collected** (cookies, donor data, data from aid and social services beneficiaries, data from individuals who subscribe to digests);
- **Rights of the data subject** (access to information, explanation of the purpose and fate of the data collected; right to rectify data, object to processing, request erasure, receive a timely and technically understandable response to requests, right to be forgotten).

In addition, the PIN website has a separate list of those who can receive information under the regulation on data retention about and for donors. It is undeniably positive that the policy is concise and understandable for the average person. At the same time, very many aspects important for data protection are not covered by the policy and an extended version is not available on the PIN website. For example, there is a lack of information on assessing the impact of policies and practices on data protection, details of data transfers to third parties, breach notification and privacy.

As already mentioned, there are no media cases related to data leaks from PIN databases. At the same time, one should be aware that the organization could easily be on the list of those whose data was leaked during the hack of the U.S. government's aid beneficiary database. However, there have been no public reports of this, so it can be presumed that PIN has been fortunate to have avoided any data security problems.

ACTED (France). This is a French organization that primarily works "in the field" and directly provides humanitarian aid to victims of war or other disasters. ACTED is also working in Ukraine providing food, clothing and other basic necessities to people in the most vulnerable regions of the country during the armed conflict. The organization also helps refugees and forecasts the development of the humanitarian situation based on the data collected.

ACTED's Data Protection Policy is very well structured, however, a bit unlike those of international non-governmental or intergovernmental organizations. However, it cannot be said that this makes it worse, rather the opposite. The organization has managed to fit into 10 pages all the information that some other institutions required 40 pages to cover:

- **The purpose and scope of the Policy** (including applicable to partner organizations);
- **Types of data most commonly collected** (name, address, means of communication, passport number, date and place of birth, information about relatives, geolocation, business contacts, fingerprints);
- **Applicable regulation** (French law, GDPR and national laws of the countries where ACTED operates);
- **Principles** (legitimate grounds for data processing, compliance with the purpose of data processing, transparency, necessity and proportionality, data privacy and security, data quality and accuracy);

- **Data processing** (consent, having a legitimate interest, telecommunications and the internet – technical requirements for the use of communication tools in humanitarian work);
- **Subject's rights** (access to information, right to request deletion of data and to object to processing);
- **Data transfer** (including as part of cooperation with law enforcement agencies, but subject to approval of the data transfer by the data protection officer within the organization);
- **Requirements for responses to data requests** (timeliness, comprehensibility, clarity and completeness, applicable to both requests from individuals and partner organizations);
- **Confidentiality and security** (including technical);
- **Breach notification and liability.**

This is one of the few policies that explicitly states that it applies to biometric data (fingerprints). Unfortunately, though, the purpose of their collection and processing is not specified. Overall, ACTED's policy is one of the most advanced in terms of data handling and processes for data transfer and processing with all the necessary safeguards in place. In addition, it is simply and clearly worded, concise and accessible to the average reader.

In addition to the Data Protection Policy, ACTED has other specialized policies, such as those on child protection, prevention of sexual harassment and sexual crimes, etc. Some directly relate to the protection of sensitive data and are important, especially as ACTED works with vulnerable groups 'in the field', operating in dangerous contexts and handling sensitive information. A separate policy also addresses data protection when using a website. However, it is "hidden" among other website use policies and is not easy to find.

No cases of data leaks from its databases have been identified. At the same time, like many other representatives of the public sector, the organization could have been on the list of those whose data was leaked during the hack of the U.S. aid beneficiary database. It should be noted that in the event of such incidents, it is important that the organization properly communicates the existence of a data protection breach.

IMPACT (Switzerland). The organization prepares analytical reports on violations of humanitarian law and the impact of armed conflicts on human rights, monitors the environment regarding humanitarian needs and develops plans for humanitarian assistance, in particular in the context of Russian armed aggression in Ukraine. IMPACT is interesting to study because, unlike PIN and ACTED, it handles personal data as a third party, having received it from other organizations that directly collected the data. This means that data protection policies must also meet international standards.

IMPACT's Data Protection Policy is slightly different in structure from the policies of organizations working "in the field", which makes sense because the purpose of the activity and the ways of working with information are fundamentally different. The only exception is ACTED, with whose policy it is very similar, because the organizations are in close partnership. Therefore, the structure and emphasis of IMPACT's policy looks similar to ACTED's policy:

- **The purpose and scope of the Policy** (including applicable to partner organizations);
- **Types of data most commonly collected** (name, address, means of communication, passport number, date and place of birth, information about relatives, geolocation, business contacts, fingerprints);

- **Applicable regulation** (Swiss law and ACTED's Child Protection Policies);
- **Principles** (legitimate grounds for data processing, compliance with the purpose of data processing, transparency, necessity and proportionality, data privacy and security, data quality and accuracy);
- **Data processing** (consent, having a legitimate interest, telecommunications and the internet – technical requirements for the use of communication tools in humanitarian work);
- **Subject's rights** (access to information, right to request deletion of data and to object to processing);
- **Data transfer** (including as part of cooperation with law enforcement agencies, but subject to approval of the data transfer by the data protection officer within the organization);
- **Requirements for responses to data requests** (timeliness, comprehensibility, clarity and completeness, applicable to both requests from individuals and partner organizations);
- **Confidentiality and security** (including technical);
- **Breach notification and liability.**

This document explicitly mentions applicability to biometric data (fingerprints), although (again) without specifying the purpose. In other respects, the IMPACT Policy (as mirrored by the ACTED Policy) is one of the most advanced in terms of data handling and processes for data transfer and processing with all the necessary safeguards in place.

In addition to the IMPACT has many other more specialized policies, such as those on child protection, prevention of sexual harassment and sexual crimes, etc. Some of these directly relate to the protection of sensitive data and are important, especially as IMPACT monitors and plans humanitarian relief actions for vulnerable groups. A separate policy has also been developed to communicate data protection rules on the website and during its use.

Given that IMPACT does not work with personal data directly, but rather receives it from other organizations for statistics, forecasting and research, it makes sense that the organization is not on the list of priority targets for hacker attacks. As a consequence, no cases of data leaks from its databases have been identified. At the same time, like many other representatives of the public sector, the organization could have been on the list of those whose data was leaked during the hack of the U.S. 's aid beneficiary database. It should be noted that in the event of such incidents, it is important that the organization promptly and properly communicates the existence of a data protection breach.

In addition, many other local organizations have very detailed data protection policies. For example, Norwegian Refugee Council has a very detailed and well-structured policy that covers both legal and some technical issues. Cyprus Refugee Council operates in a similar way, with a detailed and structured policy on the protection of personal data. Danish Refugee Council has a similar policy, which also has a list of additional internal guidelines that regulate specific aspects of data handling. In addition, the Danish Refugee Council has a special system that focuses on forecasting, for example, forced relocations and refugee crises for the next 1-3 years, which involves processing personal data on a large scale for purposes that are indirectly related to humanitarian aid. Importantly, such systems can subsequently "migrate" to the state and be used to prevent immigration, refugee influxes, or even commit crimes against humanity if regimes are prone to authoritarian practices. Therefore, extreme caution should be exercised with the transfer of such technologies.

The Danish organization Bevar Ukraine, established specifically to help victims of Russian aggression in Ukraine, has a fairly detailed policy (it is important that the policy is available in Ukrainian). Arche Nova Organisation and Equilibrium have much less detailed policies, which are also quite difficult to find through the basic navigation on the website and Google search. Finally, relatively new organizations such as Geneva Call have no privacy policy in the public domain at all. This may indicate one of two things: either the organization does not have codified policies at all, so humanitarian aid recipients cannot learn about data practices, rights, and level of protection against unauthorized access, or they are not made public on the website (which actually has the same consequences).

That is, compared to international institutions, the situation with national foreign NGOs is somewhat worse, because the level of detail of policies and their application in practice largely depends on the age of the organization, the sensitivity of the issues it works with (for example, work with refugees is traditionally considered more sensitive than local assistance, when persons are not persecuted or do not risk being expelled from the country), as well as the size of the organization. Another option, of course, could be the absence of public policies, but this is also rather a negative indicator, as it indicates the inability of beneficiaries to realize in advance where and how their data may be shared and what it may be used for. In any case, this situation should be changed.

Ukrainian local organizations

Regardless of the type and reasons for humanitarian aid, organizations working with those affected or in need of asylum must document and record the manner in which aid is provided, and therefore collect personal data. Ukrainian organizations are no exception. For example, in Chernihiv, when distributing meal kits, they registered individuals to ensure that there was enough food for everyone and collected a minimum amount of information to identify individuals. This practice is not new for other regions.

At the same time, there are many newly established organizations in Ukraine – a natural response to the full-scale invasion and the public need for humanitarian assistance, its organization and coordination. As noted, since February 24, 2022, the number of humanitarian organizations has increased fivefold compared to the period before the full-scale invasion. Newly established organizations have often focused more on the delivery of aid itself than on data protection. And the context in which they operated was clearly not conducive to changing focus or thinking about secondary things. So let's find out whether things have changed over time and whether Ukrainian organizations finally have adequate data protection policies.

Ukrainian Red Cross Society. This is one of the oldest organizations operating in the field of humanitarian issues in Ukraine. Note that the National Red Cross Society and the ICRC are not the same organization, they have different administration. Now the Society is directly engaged in humanitarian aid and has very high indicators in this field. The national organization has two types of privacy policies for donors and for beneficiaries. It is worth focusing on the second one in this study.

The notice on personal data processing is available on the organization's website and is quite brief. As the Society is registered in Ukraine, most of the Privacy Policy contains references to national legislation:

- **Types of data that are most often collected** (data of donors, volunteers, information requesters and newsletter subscribers);
- **Purpose of data processing** (keeping records of donors, selecting candidates for volunteering, providing responses to inquiries, feedback or complaints, informing about the Society's activities);

- **Applicable regulation** (Ukrainian law);
- **Subject's rights** (access to information, access to own personal data, right to request deletion, modification, destruction of data and object to its processing, right to withdraw consent to data processing, protection against automated decisions);
- **Data transfer** (employees, contractors and volunteers, national societies of the Red Cross or Red Crescent in other countries, IFRC, operators of payment systems and financial institutions, business partners, agents, professional advisers and service providers, postal marketing services);
- **Cookie files** (customizable);
- **Storage period** (as long as necessary to achieve the purpose of processing).

It is noticeable from the policy that it applies primarily to information collected via the website, while the privacy policy makes no mention of the protection of beneficiary data. In addition, there are questions about the possibility of transferring data to other National Societies, as this potentially implies that data could be transferred to Russia. At the same time, the Russian national society violates the principle of neutrality and is actively involved in an armed conflict, which puts personal data subjects at risk. In case the data is transferred to this organization, the information may get to the Russian government and be used to persecute Ukrainian citizens belonging to vulnerable groups.

There is also no mention of personal data in the Principles and Values section of the website Neither the Articles of Association, nor the Society's Strategy for 2021-2025 contain details on the protection of beneficiaries' data. There is also no information on how to handle personal data in the FAQ / Answers section, which indicates the relative impossibility for the average reader to find information on policies before directly receiving assistance. The only thing that makes it possible to understand the applicable standards is Resolution No. 487 of the Cabinet of Ministers of Ukraine on cooperation with the Red Cross, which states that the requirements of the Law of Ukraine "On the Protection of Personal Data" are applicable to the process of distributing humanitarian aid.

The Society emphasized that it conducts selective verification of persons who apply for compensation for IDP accommodation costs. This clearly indicates the processing of personal data by the organization. At the same time, some programs of the organization explicitly note the absence of requirements for the collection and processing of personal data.

The absence of codified policies or at least their absence on the website is a negative sign, also because the Society is one of the leading organizations in the humanitarian field. This, in fact, became the basis for incidents back in the days of COVID-19, when the Society was forced to debunk myths about the collection of bank card data. Also, in March 2023, the Society's website was subjected to a cyber attack, which was subsequently reported to users. However, as stated in the news story, no personal data was affected.

Another red flag was the numerous attempts to pass off as Society employees in order to steal personal data. For example, fake street advertisements for humanitarian aid. The media also reported on the creation of fake Telegram channels of the Society for the purpose of phishing and stealing subscribers' personal data. Fraud attempts were recorded, in particular, in Ternopil region. This demonstrates the need for awareness-raising and communication campaigns about what assistance from the National Red Cross Society really looks like.

MacPaw Development Foundation. This is a charitable foundation founded by a Ukrainian IT company that has been involved in aid since 2016, and after the full-scale invasion it refocused on helping those affected by Russian aggression. The foundation has a privacy policy that applies to any data collected by the organization.

The Privacy Policy applies to the website and the data collected through it. Much of the Privacy Policy contains references to national legislation:

- **Types of data that are processed** (contact data, technical details, details of the website use);
- **Inapplicability to persons under 13 years of age;**
- **Applicable regulation** (Ukrainian law and GDPR);
- **Subject's rights** (access to information, right to request deletion, modification, destruction of data and object to its processing, right to withdraw consent to data processing);
- **Data transfer** (only to law enforcement agencies upon lawful request);
- **Cookie files** (customizable);
- **Data leakage** (obligation to report).

Unfortunately, the policy lacks information on the rights of users to submit a request to change or delete data, as well as the possibility to withdraw consent to data processing.

Center for Civil Liberties (hereinafter referred to as the CCL). It is a Ukrainian human rights organization, which won the Nobel Peace Prize and operates mainly in the analytical area, similar to the already analyzed IMPACT organization. It analyzes personal data for the purpose of forecasting, analytics or research.

The Privacy Policy applies to the website and the data collected through it. Much of the Privacy Policy contains references to national legislation:

- **Types of data that are most frequently collected** (completed forms, bank transfers and cookies);
- **Purpose of data processing** (selecting candidates for volunteering, providing responses to inquiries, feedback or complaints, informing about the activities, public acknowledgments);
- **Applicable regulation** (Ukrainian law);
- **Data transfer** (only to law enforcement agencies upon lawful request);
- **Cookie files** (customizable).

Unfortunately, the policy lacks information on the rights of users to submit a request to change or delete data, as well as the possibility to withdraw consent to data processing.

In contrast to the CCL, other similar NGOs such as ZMINA, Human Rights Platform, CHESNO Movement, which also work on creating analytical products and may sometimes receive personal data of beneficiaries for research purposes, do not have privacy policies either for dealing with such issues or for their own website. This is a rather unfortunate situation, especially given that some of these organizations work directly with data protection issues.

Other organizations that directly or indirectly assist or are philanthropists whose work is related to the armed conflict are Voices of Children CF, Alliance for Public Health, Dobrodiy Club CF, Right to Protection, Caritas Ukraine, Rokada, Educational Human Rights House in Chernihiv, Educational Human Rights House in Chernihiv ICF, Proliska, The Tenth of April. They do not have privacy policies even for the website (while privacy policies for "in the field" work either do not exist or are not publicized). Some organizations, such as the Volunteer Hundred of Dobrovolia, operate primarily through Facebook, where privacy policies (and finding them) are even more difficult. Others, like Stabilization Support Services, have a very extensive system of policies that

lacks only a data protection policy. It is a shame that even organizations that have been operating much longer than the full-scale invasion and have been dealing with humanitarian aid for a long time do not have policies published on their own websites, including CrimeaSOS, DonbasSOS and VostokSOS.

There are also negative cases at the local level – in matters of direct provision of humanitarian aid. For example, Brovarska Hromada NGO got involved in a scandal due to excessive collection of personal data. Thus, the organization required TIN, as well as data on the number of family members and their contact information, which is clearly not proportional, for example, when it comes to one-time financial assistance. Regarding such cases, expert **Oleksii Kabanov** notes that these situations are not sporadic, rather it is a common practice for Ukrainian context. The expert adds:

> ***«...humanitarian organizations, especially small ones, do not have approved procedures for processing personal data. ...I think it is not difficult to find posts on Facebook that are circulating around the network, with excessive data on missing persons and their relatives. As a rule, the families of such persons become victims of either hostile well-wishers or fraudsters. The numbers of relatives, bank account details, data about the missing person (date of birth, what the person enjoyed doing, who his/her friends were, where he/she served, what he/she did, photos with relatives, etc.) are often made public.»***

Other organizations, such as Association Internationale de Cooperation Medicale, in response to the UMDPL's request, explicitly stated that they do not share any information about work in Ukraine for security purposes. On the one hand, it's positive that the organization is open to communication, but on the other hand, it doesn't help beneficiaries understand how safe they will be if they go to such a charity.

There are also a number of state and semi-state programs focused on facilitating access to humanitarian aid. These include YeDopomoha and SpivDiia. Both initiatives have fairly detailed policies, which can be found at the respective links (first and second). Unfortunately, the YeDopomoha Policy pays little attention to the protection of personal data, and therefore most of the traditional rights of subjects when registering for aid are not actually provided for in this document. This is also a problem, because state initiatives are often perceived by private organizations as a benchmark. When public initiatives lack a responsible attitude towards the development of privacy policies, the private sector may perceive this as a green light for such an attitude.

The brief conclusions can be considered rather disappointing: Most national humanitarian organizations do not have data protection policies on their own websites. Consequently, citizens in need of assistance are not able to properly familiarize themselves with their own rights, to foresee where and how data can be transferred. In this regard, Tetiana Oleksiiuk, an expert in the field of personal data protection, bluntly noted that the public sector rarely familiarizes the beneficiaries with privacy policies. She also emphasized:

> ***«....it should not be expected that humanitarian aid beneficiaries (and these are people in difficult life circumstances and vulnerable people) will feel confident enough to insist on compliance with the requirements to protect their personal data. For people on the brink of survival, this doesn't seem like a priority».***

Vitalii Moroz, a digital rights expert, also adds from his experience of interacting with the public sector that organizations, unfortunately, very rarely have detailed data protection policies, because this requires awareness of the topic of data protection, constant legal support of this issue and a desire to prioritize this area in the activities of the organization. According to the

expert, often humanitarian organizations do not even have privacy policies on their websites, let alone separate data protection policies for aid.

Therefore, unfortunately, the culture of personal data protection in Ukraine is not very high, however, human rights organizations are exactly those actors who should take into account the dangers associated with data leaks and hacker attacks; especially those organizations that are registered and operate in Ukraine, and therefore are naturally at a higher risk due to Russian aggression.

SECTION V.
Recommendations

Protection of personal data during the armed conflict is not only the task of humanitarian organizations, every stakeholder should be involved in this process. In particular, because the policies of organizations often depend on national regulation, and the practice of work with personal data protection on the beneficiaries' awareness of their rights, the willingness of other human rights organizations to monitor compliance with standards, as well as the level of technical and legal expertise of supervisory authorities. That is why the protection of personal data in the provision of humanitarian assistance should be approached in a comprehensive manner. The analysis of international and national standards, policies and practices of humanitarian organizations has led to a number of recommendations presented below.

For national governments:

- Develop foreseeable national legislation that will adequately regulate the collection and processing of personal data, including for humanitarian purposes (e.g., provide for the applicability of the Law of Ukraine "On the Protection of Personal Data" to the activities related to the provision of humanitarian assistance in the relevant law).

- Update the outdated legislation on personal data protection in case it does not comply with applicable international standards, does not provide for framework restrictions on the use of automated technologies or safeguards against their abuse (e.g. automated decision-making, systems controlled by artificial intelligence, etc.).

- Ensure that humanitarian organizations can easily and quickly communicate with governmental agencies responsible for data protection and make it possible to clarify national standards to foreign organizations.

- Communicate with donor agencies to reduce the requirements on the transfer of large amounts of personal data from recipient humanitarian organizations as reportable information. Clarify the sensitivity of the contexts in which humanitarian organizations operate.

- Communicate state database hacks and data breaches so that humanitarian organizations have an understanding of the personal data security situation in the region and directly in the states where they are registered or assisting.

For humanitarian organizations:

- Develop data protection policies where such policies do not exist. Update outdated or irrelevant policies and adapt them to the context of the humanitarian organization's work and the technologies it uses to collect and process data.

- Post policies in a prominent place on the organization's website, make them easily accessible to potential beneficiaries, and communicate updates in a timely manner.

- State in the policy that it applies to all data processing that the organization undertakes, or if the policy applies only to data collection through the website, clearly mention this in the title of the policy and provide a link to the policy that applies to other data collections, in particular humanitarian assistance processes.

- Draft policies in clear language and keep them short and concise (e.g. the UN World Food Program's 130-page policy is clearly not conducive to familiarizing ordinary beneficiaries in critical situations).

- Develop a version of the policy in child-friendly language if the organization's focus is on working with and providing humanitarian assistance to children.

- Clearly and comprehensively describe in the policy the list of data to be collected and the purpose of collecting specific categories of data (in particular, this will help humanitarian organizations themselves to ascertain whether they are collecting excessive amounts of data and whether the amount of data is proportionate to the purpose).

- Conduct regular risk assessments of activities to protect personal data, reviewing data protection policies depending on the context of the work, the type of humanitarian assistance provided and the data processing tools used by the organization:
  - The assessment should be carried out before, during and after the provision of humanitarian assistance;
  - The assessment should be based on the level of risk from a particular activity, the use of a particular technology or a particular action in a particular context;
  - The assessment should focus on a "privacy by default" approach;
  - The assessment should take into account the technological development of society and the effectiveness of technology to overcome specific challenges;
  - The assessment should have a practical rather than formal meaning.

- Avoid overly broad grounds for data collection and processing when drafting personal data protection policies, in particular not to include "public interest" or "legitimate organizational interest" to the grounds for data processing without adequate detail.

- Minimize data collection, especially in cases where the organization is small in terms of staff and expertise or unable to fully ensure data security from a technical and legal point of view. This is especially true if the organization plans to collect biometric data or is working with technologies that require significant technical expertise.

- Provide refugees and asylum seekers with access to data about them, explain the purpose of the collection and how the data will be processed, the fate of this information. If there is an error in the data, provide an opportunity to correct the information.

- When using third-party resources (software, apps or websites, such as the ICRC's Trace the Face) to identify individuals, create databases or for other purposes related to humanitarian assistance, post data protection policies on such resources, make them clear and concise, where possible adding the languages of the region with which the humanitarian organization actively works.

- Refrain from sharing data with the state or other actors, especially when doing so without warning the individuals whose data is to be shared. In the case of vulnerable groups that may be discriminated against in the state in which humanitarian assistance is provided, maintain maximum confidentiality in communications with the public sector.

- Carefully weigh the risks of handing over systems for predicting waves of migrants, refugees and others in need of humanitarian assistance to the state (in particular, as was the case with the system developed by Danish Refugee Council). This is particularly important in the context of working in non-democratic regimes, where the state may seek to exchange

authorization to work in the region for access to technology.

- Designate a person responsible for data protection and post the contacts of such a person on the website to enable communication between any stakeholders and the data protection expert within the humanitarian organization.

- Clearly state the rationale for collecting biometric data and the extent to which it helps to avoid fraud, improve identification processes and reduce the costs of humanitarian assistance (including financial and technical calculations and performance indicators for available alternatives to personal data collection).

- Strengthen legal and technical personal data skills for humanitarian organization staff who work directly or indirectly with data. In particular, educational programs and certifications offered by the ICRC and academic institutions may be helpful.

- Utilize password administration applications for enhanced security, which can safeguard against the use of stolen personal data or hacked accounts for illegal activities.

- To avoid data breaches and system hacks, install software to apply security updates, and conduct regular audits to assess system vulnerabilities (test new systems and verify the ability of older systems to withstand new challenges and threats).

- Develop crisis protocols in case of hacks or attacks that will contain a clear algorithm of actions for members of the organization involved in the handling of personal data, regularly review and update such protocols depending on the working environment and applicable data processing technologies.

- In the event of a cyberattack or data breach, communicate in a timely manner with those whose data may be or have been compromised about the existing threat, analyze security gaps and update / strengthen / modify policies as necessary.

- Refrain from the use of media like Telegram, Facebook or other insecure social networks and messengers to collect data.. Use communication channels that contain peer-to-peer connection and the ability to delete correspondence from the server to maximize privacy.

For donor organizations:

- Incorporate data protection into project planning and reporting forms, taking into account the sensitive contexts in which organizations implementing humanitarian projects typically operate.

- Adhere to the principle of data minimization and refrain from requesting excessive amounts of sensitive information (in particular, do not request information on gender, sexual orientation, origin, belonging to marginalized or vulnerable groups, etc.).

- Be flexible and adaptive when the direct aid provider notes the particular sensitivity of the data received and refuses to include such information in reporting forms.

- Review technical standards for the transfer of data from the humanitarian to the donor organization and strengthen data protection where there are doubts about the reliability of communication channels. If this is not possible, refuse to transfer particularly sensitive categories of data.

For humanitarian aid beneficiaries:

- Use the initiatives developed to protect the rights of Ukrainians from human rights organizations, information resources and guides on how to receive aid (like the EU Solidarity with Ukraine page).

- Be careful when providing personal data to receive humanitarian aid or participate in so-called population censuses in the occupied territories, avoid disclosing information about military personnel, their family members, civil activists, journalists, and public figures.

- Avoid websites or digital applications that are not secure. At least avoid using such applications to transmit personal data.

- Be attentive to e-mails from unknown recipients, messages in messengers (Viber, Telegram, WhatsApp) from unknown phone numbers, as well as messages on social media (Facebook, Instagram) from unknown users, never open suspicious links and files.

- Whenever possible, use two- or multi-factor authentication when authorizing in information systems, websites, accounts and follow other digital security rules. They can be found on the Yak? resource.

- Be careful when scanning QR codes to perform any actions related to providing personal data, receiving assistance or information about providing assistance, because QR codes can lead to unverified links and, as a consequence, to downloading malicious software and data theft from the device.

- Refuse to share personal data, including account passwords, one-time passwords, geolocation data, etc., with third parties until there are legitimate and necessary grounds for collecting such information.

- Refrain from providing your personal data and consent to their processing until you have familiarized yourself with the purpose and grounds for the processing of personal data, as well as the conditions of their processing (in particular, familiarization with privacy policies), unless the relevant processing is carried out on the basis of the law for the performance of the data owner's duties.

- Send requests for information on the sources of collection, location of personal data, purpose of processing, location of the personal data owner or controller.

- Submit a reasoned request to the personal data owner objecting to the processing of his/her personal data, modification or destruction of his/her personal data, if such data is processed unlawfully or is incorrect.

- Withdraw consent to the processing of personal data (if consent has been granted).

- Use reliable sources for information, e.g. IMI monitoring provides a list of conscientious media outlets that adhere to journalistic standards.

- Participate in the development of data protection policies at the level of the state, humanitarian and donor organizations, share experiences regarding problems that have arisen in practice in receiving humanitarian aid, propose solutions to strengthen data protection, improve privacy policies, etc.

For human rights organizations:

- Contribute to raising awareness among humanitarian organizations about the rules of personal data handling, as not all humanitarian organizations are human rights organizations and therefore may lack both legal and technical expertise.

- Share good practices on data protection (including formulations of policies), secure data collection and transfer to third parties (where appropriate), and report on negative experiences to avoid similar situations in the work of other organizations.

- Condemn cases of personal data breaches, disregards for technical security, abuses or manipulations on the part of beneficiaries due to the more privileged position of the humanitarian organization (as a resource manager).

- Communicate problematic data protection cases and potential solutions to the state (regulatory policies and reporting), donor organizations (reports and volumes of data), humanitarian organizations (potential change in practices), citizens (increased digital literacy, ability to protect their own personal data).

For the media:

- Refrain from spreading unverified allegations of data breaches by humanitarian organizations, as false information can undermine credibility in the humanitarian sector, causing aid to be denied to those in need.

- Contact organizations that may have experienced a data breach or whose databases may have been the subject of a hacker attack to verify information and gain a broad perspective on the issue.

- Refrain from exaggerating the consequences of data breaches or cyberattacks (e.g., a DoS attack is not equal to a database breach, so the damage to personal data will be much less, if not zero, so they should not be equated).

- In case of a data leak to the network, refrain from further dissemination of personal data and increasing the audience with access to sensitive information.

- Promote campaigns aimed at raising awareness of data protection rules among citizens and programs to develop the capacity of humanitarian organizations to protect personal data (trainings organized by the state, other NGOs, academic community, etc.)