



Compliance Report

Documenting international crimes and human rights violations for accountability purposes: Guidelines for civil society organisations

drafted by
Kaja Kowalczywska Ph.D.

November 2023

Table of contents

1	About Foundation Sunflowers.....	2
2	Methodology of the Project Sunflowers	3
2.1	Mission	3
2.2	App-like form	3
2.3	Volunteers.....	4
2.4	Awareness raising	4
2.5	Vulnerable persons	4
2.6	Exclusions: our boundaries and limitations.....	4
3	About Guidelines	5
4	The aim of the Compliance Report	5
5	Introductory Remarks	6
6	General Principles.....	6
6.1	Do no harm.....	6
6.2	Informed consent.....	8
6.3	Objectivity, impartiality and independence	8
6.4	Accountability and legality.....	9
6.5	Professionalism and respect.....	10
7	Planning and Preparation	10
7.1	Early preparation.....	10
7.2	Resources.....	11
7.3	Security.....	11
7.4	Confidentiality	12
7.5	Vicarious trauma	13
7.6	Vulnerable persons	14
8	The Foundation’s Method of Collecting Information.....	15
9	Storing and Safeguarding	17
10	Annexes	18
11	Recommendations Summary	19

1 About Foundation Sunflowers

The Foundation Sunflowers is a non-profit organization that was established on July 25, 2022, and operates under the most current version of its statute adopted on February 2, 2023. With its registered office located in Warsaw (01-203), at ul. Siedmiogrodzka 5/51, 01-204 Warsaw, Poland, and registered under the number 0001019393, the foundation is dedicated to addressing issues related to international crimes and human rights violations.

The primary mission of the Foundation Sunflowers revolves around several key objectives:

- a) **Supporting Efforts to Collect Information on Evidence of International Crimes:** The foundation is committed to gathering and documenting information on international crimes, with a particular focus on crimes committed in Ukraine since February 24, 2022.
- b) **Supporting Victims of International Crimes in Obtaining Remedies and Reparation:** The Foundation Sunflowers seeks to assist victims of international crimes in their pursuit of justice and reparation for the damages and harm they have suffered.
- c) **Increasing Public Legal Awareness of Responsibility for International Crimes and Victims' Rights:** The foundation aims to educate the public about the responsibility for international crimes and the rights of victims affected by such atrocities.
- d) **Promoting and Protecting Human Rights and Freedoms:** The Foundation Sunflowers is dedicated to promoting and safeguarding human rights and freedoms, contributing to the development of democracy.
- e) **Provision of Free Civic Consultancy:** The foundation provides free-of-charge civic consultancy services to individuals and groups seeking guidance on legal and humanitarian matters.
- f) **Promotion and Organization of Voluntary Work:** The Foundation Sunflowers actively encourages and coordinates voluntary work to address various humanitarian and human rights issues.

The Foundation Sunflowers, has a core initiative called "Project Sunflowers." Our primary focus is on the security and confidentiality of the information entrusted to us. We take great care in diligently collecting and storing this information, with the sole purpose of passing it on to competent authorities who have the power to prosecute crimes committed in Ukraine since February 24, 2022. Moreover, we collaborate closely with authorities responsible for developing reparation programs to provide support to the victims affected by these crimes in the future.

It is of utmost importance to us that the information shared with our foundation is used solely for these purposes, ensuring the trust and confidentiality of those who seek our assistance. As of October 2023 we became a member of the **Coalition for International Criminal Court**.

In summary, the Foundation Sunflowers plays a crucial role in advocating for justice, human rights, and the well-being of victims impacted by international crimes. We are dedicated to maintaining transparency, confidentiality, and the responsible handling of information, which reflects our unwavering commitment to creating a safer and more just world.

2 Methodology of the Project Sunflowers

2.1 Mission

The Project Sunflowers primary scope of activities revolves around the critical task of **storing and safeguarding information pertaining to evidence of crimes and damages**. We focus on preserving crucial data related to such incidents, ensuring its confidentiality and integrity. Our uniqueness lies in being composed of an international team of experienced lawyers. This diversity of expertise enhances the strength of our organization. Furthermore, our global implementation through a network of volunteers enables us to reach far and wide, collecting information from potential witnesses and victims. This information is then **carefully stored in our secure database and subsequently shared with relevant international and national law enforcement authorities, tribunals, and courts, as well as authorities responsible for reparations programs for survivors**.

Our guiding principle is encapsulated in the phrase "**Enabling Information, Enabling Justice**."

2.2 App-like form

To support our mission, we have developed an app-like form that efficiently collects relevant information, all of which is securely stored on our cloud. **The process of taking a person's account is carried out through an online app that is exclusively filled out by the individual themselves. Additionally, each person filling out the form may upload any pictures or videos they possess, depicting the events described in the form or the damages suffered**. Our volunteers merely provide guidance on the procedure but do not have access to the information stored in the database. The collection of information strictly

adheres to the principles of free and informed consent, allowing the person to withdraw their consent at any time if they choose to do so. The information in the database is stored indefinitely. The justification for this storage is the non-expiry of the prosecution of war crimes, crimes against humanity, genocide, and crimes of aggression.

2.3 Volunteers

Our dedicated volunteers are **extensively trained to assist potential witnesses and victims in providing essential information about the crimes committed in Ukraine and the damage resulting from this armed conflict**. Through specialized training in psychological support, our volunteers are equipped to sensitively interact with individuals who have been traumatized by war, ensuring a compassionate and supportive environment.

Our network of volunteers spans across many countries, including Poland, Ukraine, Slovakia, Czech Republic, Germany, the Netherlands, Belgium, Ireland, the UK, France, Spain, Italy, Greece, Bulgaria, Sweden, Estonia, the USA, Lithuania, Hungary and Canada. This **global presence** sets us apart and strengthens our outreach and impact.

2.4 Awareness raising

In addition to this crucial mission, we take pride in our efforts to raise awareness about various critical issues. We focus on shedding light on international war crimes, crimes of genocide, crimes against humanity, and crimes of aggression. Moreover, we emphasize the importance of humanitarian law, migration law, human rights, and the reparations process for victims of armed conflict.

2.5 Vulnerable persons

During the process of information collection, **we avoid involving vulnerable individuals, including children under the age of 13**. However, if our volunteers notice signs of trauma and identify the potential risk of re-traumatization, they are instructed to provide the individual with contact information for a specialist who has been vetted by the Foundation. This specialist is qualified to offer the necessary medical and psychological support to the individual.

2.6 Exclusions: our boundaries and limitations

It is essential to emphasize that we do not engage in any form of personal intrusion, either in person or remotely. Our interactions with individuals are

strictly limited to guiding them about the Project's rules and aims, without direct engagement in questioning. Moreover, we do not capture videos or photos, store physical items, or document any unrelated digital information. Online investigations, documenting physical injuries, and crime scenes are beyond the purview of our responsibilities. Additionally, the analysis of collected information falls outside our mandate. Consequently, chapters 5-11 of the Guidelines do not directly apply to our specific activities, as we adhere to a distinct and specialized focus on information preservation and security.

3 About Guidelines

In an effort to bolster accountability and promote justice for international crimes and human rights violations, **Eurojust and the International Criminal Court** have jointly developed comprehensive guidelines titled "Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations", reference: DOI 10.2812/682168 (hereinafter referred to as "Guidelines"). Available at: www.eurojust.europa.eu/publication/documenting-international-crimes-and-human-rights-violations

The purpose of the Guidelines is to provide support to civil society organizations in their efforts to gather and preserve information concerning international crimes and human rights violations. **The aim is to ensure that such information can be admissible as evidence in a court of law.** The Guidelines consist of a set of **suggested actions and precautions, outlining what actions might be beneficial and what could potentially hinder criminal accountability endeavors.**

These Guidelines have been formulated in response to requests from multiple civil society organizations and stakeholders in the accountability field. They expressed a need for guidance to ensure that the information they collect holds the potential to be utilized as evidence in future prosecutions, whether at the national or international level.

4 The aim of the Compliance Report

This compliance report has been prepared with the primary aim of **evaluating the extent to which the Foundation Sunflowers aligns with the criteria stipulated in the Guidelines.** The assessment seeks to ascertain the

Foundation's adherence to the prescribed guidelines and to identify areas where additional measures may be required to bolster its readiness in fulfilling its mission.

5 Introductory Remarks

Some on-ground activities carry the risk of being harmful or detrimental to criminal accountability endeavours. Civil society organizations cannot substitute or replace the actions of competent investigative authorities, whose mandate is to enforce the law. Although civil society organizations may have good intentions in their documentation efforts, they can undermine accountability mechanisms if they fail to adhere to essential standards. The coexistence of numerous civil society organizations and stakeholders within the same accountability sector, employing different standards and tools, can lead to over-documentation, elevate the risk of re-traumatization, and potentially compromise the quality of evidence available for accountability purposes.

For this reason, civil society organizations engaged in documenting international crimes and human rights violations are strongly encouraged to incorporate the Guidelines into their standard practices.

Recommendation: As of the present moment, the Foundation has formulated its mission and activities leveraging the knowledge and expertise of its founders. Nevertheless, it is imperative to note that there are currently no documented standards and procedures in place.

The Foundation Sunflowers should carefully consider the importance of implementing a standardized documentation procedure that incorporates all these guidelines.

Currently, the volunteers are undergoing training in these procedures. It should be considered to develop a knowledge base, also in documented form, to facilitate knowledge sharing and enhance procedural transparency.

6 General Principles

6.1 Do no harm

This principle emphasizes the responsibility of the Foundation to **proactively prevent or minimize any unintended negative impacts of their documentation activities on both others and themselves**. All such activities

should consistently prioritize the best interests of individuals providing information, intermediaries, local communities, and any other participants involved in the documentation process. By adhering to these ethical guidelines, organizations can ensure that their documentation efforts remain sensitive, respectful, and beneficial to all stakeholders, fostering a more responsible and inclusive approach to their work.

To fulfil these principles, the Foundation needs to undertake various actions **before, during, and after the documentation process**, which include:

- Conducting risk assessments
- Providing training and carefully selecting staff to uphold professional standards of conduct
- Obtaining informed consent from individuals involved
- Ensuring the protection of sources and respecting confidentiality
- Establishing referral support systems
- Applying specific measures to address the needs of vulnerable individuals.

It is advised that when questioning individuals, the Foundation should aim to **refrain from eliciting detailed accounts of their knowledge of crimes**. Instead, priority should be placed on **identifying the topics** on which a person may have relevant information. The primary goal should be to **record the contact details of the person**, enabling and facilitating a future interview by the competent investigative authorities.

Recommendation: Presently, the Foundation diligently adheres to the "do no harm" principle, which is meticulously integrated into various actions conducted before, during, and after the documentation process. The app's questionnaire has been meticulously crafted to allow individuals providing accounts the freedom to disclose details of crimes committed and damages endured, while also collecting their contact information. Nevertheless, given the expanding nature of the database, it is of utmost importance to undertake a thorough reassessment of potential risks and perpetually monitor actions that warrant attention, amenable to modification to better align with the "do no harm" principle.

Among the actions that necessitate focus in adherence to the "do no harm" principle, emphasis should be placed on the robustness of the referral support system and meticulous care for vulnerable individuals. Additionally, the stability and security of the database demand heightened scrutiny to ensure the protection of sensitive information and to uphold the integrity of the Foundation's mission in safeguarding the well-being and rights of all participants involved.

6.2 Informed consent

Before engaging in any information-gathering activities that involve other individuals or entities, such as conducting interviews, capturing photos/videos, or receiving documents, the Foundation should ensure that it obtains informed consent from the respective person or entity. It is essential to secure explicit permission from those involved, demonstrating a commitment to ethical practices and respecting the rights and privacy of all parties during the information-gathering process.

The Foundation has developed its own declaration of voluntary submission (Annex 1), meticulously designed to align with both national and EU laws, ensuring compliance with **the General Data Protection Regulation (GDPR)**. The Foundation developed as well the Privacy policy (Annex 2) and the Terms of service (Annex 3). Therefore the Foundation's documentation on processing personal data as well as declaration of voluntary submission, along with its handling, adheres to all the **prescribed standards of informed, contemporaneous, voluntary, and explicit consent**.

6.3 Objectivity, impartiality and independence

Objectivity is a fundamental aspect of our approach, driven by the commitment to seek the truth without making any assumptions. We ensure equal consideration of both incriminatory and exculpatory information. In the pursuit of comprehensive understanding, we examine multiple hypotheses and theories, continually reviewing and planning our activities as new information is collected. Our interactions with information providers are conducted with utmost integrity, avoiding any influence through leading questions. Furthermore, we focus solely on gathering factual information, refraining from applying legal assessments during this process. As we collect information, we meticulously evaluate the sources to test and confirm its reliability, ensuring a rigorous and impartial documentation process.

Impartiality is a guiding principle that underpins all our actions. We maintain a neutral stance and do not take sides in any matter. Our commitment to impartiality ensures that we remain unbiased and unprejudiced throughout our work. We are mindful of our cultural and personal biases and take proactive steps to mitigate their influence. Our working methodologies are designed to encompass all relevant facts and information, ensuring we avoid any 'tunnel vision' or 'confirmation bias' that might hinder objective analysis. Furthermore, we

are vigilant in identifying and avoiding any conflicts of interest, thereby upholding the highest standards of integrity and fairness in our endeavours.

Independence is a core value that guides our actions. We conduct our activities free from any external interference or influence, ensuring complete autonomy in our endeavours. Our commitment to independence allows us to maintain objectivity and integrity throughout our work, free from the presumed or known wishes of any person or authority. We are vigilant in identifying any organizations or individuals attempting to manipulate or disseminate false information to undermine our documentation efforts. By remaining aware of such attempts, we safeguard the credibility and reliability of the information we collect, preserving the trust placed in us by those we serve and the broader community relying on our documentation initiatives.

Recommendation: The principle of objectivity, impartiality, and independence should be incorporated into the documented standards, upheld during all activities, and consistently reminded to all volunteers.

6.4 Accountability and legality

The Foundation operates with a strong awareness of potential liability under relevant laws, particularly in the country where it conducts its activities. We understand the importance of maintaining compliance with applicable legal frameworks to ensure responsible and ethical practices in our work.

Furthermore, it is essential to clarify that **our representatives do not directly collect information**. However, they may be called upon to testify in any future proceedings related to the information gathered by our organization. In such instances, they may need to provide testimony on the reliability and authenticity of the information collected. The Foundation takes utmost care to ensure that the information contained in its records is kept confidential and secure. Safeguarding the privacy and security of the data we handle is of paramount importance to us. We employ robust security measures, adhering to best practices in data protection, encryption, and access control to prevent unauthorized access or disclosure of sensitive information.

Recommendation: The Foundation should maintain a detailed record of methods and procedures for preserving and collecting information.

6.5 Professionalism and respect

The Foundation's approach is characterized by **unwavering professionalism, integrity, respect, and empathy**. We place great importance on being mindful of cultural sensitivities and vulnerabilities, recognizing the potential impact of our conduct on those with whom we interact. Our commitment to upholding these values ensures that we engage with individuals and communities in a responsible and ethical manner, fostering an environment of trust and understanding.

As part of our ethical practices, **we strictly refrain from offering any form of remuneration or payment in exchange for information**. This principle ensures the integrity and credibility of the information we gather, allowing us to maintain an unbiased and objective approach to our documentation efforts.

Recommendation: These principles should be incorporated into the documented standards, upheld during all activities, and consistently reminded to all volunteers.

7 Planning and Preparation

7.1 Early preparation

After conducting research on the initial idea and the operational environment, the initiators of the Foundation meticulously defined its mandate, objectives, and focus. These crucial elements were then formally documented and incorporated into **the Foundation's Statute**.

Due to limited resources and mapped priorities, it became evident that the Foundation's **focus should be on providing a tool for individuals giving accounts rather than collecting the accounts through volunteers**. As a result, volunteers are primarily present to assist individuals in the process of giving their accounts. Volunteers also serve as the primary security checkpoint, as they are required to authenticate the identity of individuals providing information and to safeguard the database against unauthorized access by the general public and malicious hackers.

By adopting this approach, the Foundation can achieve its mission without incurring undue costs and burden. Moreover, this methodology ensures the interests of justice are safeguarded, allowing the Foundation to effectively pursue its objectives while providing valuable support to those who seek to share their experiences.

7.2 Resources

The Project's team comprises experienced legal professionals, including judges, attorneys-at-law, legal scholars, and investigators, each possessing distinct expertise in the fields of international criminal law, human rights, migration, and public law in a broader context. This team is characterized by its diversity, taking into account both gender and nationality perspectives, and it encompasses both professionals and volunteers. All members of the Project's team possess the requisite skills and competencies, and they undergo specialized training in the technical, linguistic, and psychological aspects relevant to the Project.

7.3 Security

The Foundation has a clear understanding of the risks associated with collecting and preserving information on evidence. As a result, during the mapping and planning of its activities, a strategic decision was made to limit its operations to primarily assisting individuals giving accounts who are located outside of the conflict zone. This deliberate approach significantly reduces the level of risk involved. By focusing on **supporting individuals outside the conflict zone**, the Foundation can effectively mitigate potential hazards while still fulfilling its mission to aid those seeking justice and accountability.

Furthermore, the Foundation has developed a method for contacting individuals by utilizing previously established connections and trust. This approach ensures **a safer environment for those giving their accounts**, as the Foundation recognizes the importance of lowering the risk of retaliation, intimidation, threats, and punishments.

The Foundation places a strong emphasis on maintaining the confidentiality of the process and the information gathered. To achieve this, stringent measures are in place.

Firstly, **no one from the Foundation has access to the content of the account, and the information can only be transferred to competent authorities upon their official request.**

Secondly, within the Foundation, access to different information is granted based on specific needs, following **the principle of minimal exposure.**

Thirdly, upon submission, the data collected from the forms is **stored in two distinct databases**: a content database, where the information from sections B and C of the form is preserved, and a personal contact database. The latter is made

available to the authorities who, after conducting an internal analysis of the information within the factual database, seek to establish contact with the individuals who have furnished pertinent information.

By implementing such stringent protocols, the Foundation takes diligent steps to protect the safety and well-being of those involved, ensuring that their trust in the organization is well-placed and their accounts are treated with utmost care and confidentiality.

7.4 Confidentiality

The security of the data stored is ensured through a comprehensive set of measures, designed to protect **the confidentiality, integrity, and accessibility of the information**. These measures include:

- **Data Encryption:** All sensitive data is encrypted to prevent unauthorized access and ensure that the information remains secure, even in the event of a breach.
- **Access Control:** Strict access controls are implemented, granting permissions only to authorized personnel based on their roles and responsibilities. This restricts access to sensitive data to only those who need it for their designated tasks.
- **Secure Storage:** The data is stored in highly secure and monitored environments, employing state-of-the-art infrastructure to safeguard against physical and virtual threats.
- **Regular Backups:** Regular data backups are performed to prevent data loss in case of any unexpected incidents.
- **Security Audits and Monitoring:** Continuous monitoring and regular security audits are conducted to identify and address potential vulnerabilities promptly.
- **Employee Training:** Staff members are regularly trained on data security protocols and best practices to enhance awareness and adherence to security measures.
- **Incident Response Plan:** A well-defined incident response plan is in place to swiftly and effectively handle any security breaches or incidents.

The Foundation has implemented the GDPR documentation and standards. The Project's team is also offered the GDPR training by legal office responsible for the GDPR compliance.

By implementing these robust security measures, the Foundation ensures that the data it stores remains well-protected and that the privacy and confidentiality of all stakeholders involved are maintained at the highest level possible.

Recommendation: the Foundation should ensure that all team members, intermediaries and interpreters are trained in and comply with confidentiality requirements and information protection protocols. The GDPR documentation should be regularly implemented and each new Project's member should be trained on GDPR compliance procedures.

The Foundation should prioritize the implementation of access monitoring to track and record user logins, including information on who logged on, when they logged on, and what resources they accessed. This measure will enhance the security and accountability of the organization's information systems.

At a later stage, particularly when sharing information with enforcement authorities, the Foundation should consider the development of a dedicated module for managing and controlling access privileges. Additionally, the implementation of Multi-Factor Authentication (MFA) to verify the identity of users accessing the system should be explored. It's important to note that these advanced security measures may not be required at the initial stage of information request, where volunteer verification of individual identity is deemed sufficient. However, as the Foundation's operations expand and involve sensitive data sharing, enhancing security with MFA and access control becomes increasingly important.

7.5 Vicarious trauma

The method of implementation of the Project Sunflowers significantly reduces **the risk of vicarious trauma by ensuring that volunteers do not have access to the accounts**. Nevertheless, while the possibility of vicarious trauma cannot be entirely eliminated, the Foundation takes proactive steps to address this concern.

The Foundation's approach emphasizes mindfulness and awareness regarding the potential impact of exposure to violence, suffering, and trauma inflicted on others. We recognize that individuals who work closely with victims and witnesses of such events may also experience vicarious trauma. As part of our commitment to safeguarding the well-being of our team, we conduct thorough research and encourage heightened self-awareness among our staff. **We strive to be well-informed about the signs and symptoms of vicarious trauma in ourselves and our colleagues, ensuring that we can identify and address any related challenges promptly and supportively.** By nurturing a culture of empathy,

support, and mental well-being, we promote a healthy and resilient team, enabling us to effectively fulfil our mission with compassion and integrity.

Hence, we conduct **training sessions for our volunteers** to ensure they are well-prepared for interacting with diverse individuals and emphasize **the importance of self-care for their mental well-being**. Additionally, we perform a comprehensive **mapping of psychological support centres** in the countries within the Project's scope. This enables our volunteers to provide individuals with specific information regarding professional assistance available in their respective countries. To date, we have successfully mapped such support centres in Poland, Ukraine, Hungary, and the Netherlands.

Recommendation: The Foundation should maintain an ongoing commitment to monitoring vicarious trauma-related concerns and proactively address requests for additional training or assistance in locating support resources, such as supervision.

Furthermore, the Foundation should persist in expanding its network of contacts with centres that provide psychological support, with a particular emphasis on the countries where our volunteers and contributors are situated. Foundation should define coping measures within its team, and identify services and professionals who can provide support when necessary.

7.6 Vulnerable persons

As a fundamental rule, **the Foundation aims to avoid its engagement with vulnerable persons**, specifically for the purpose of documenting international crimes and supporting criminal accountability mechanisms, to the minimum extent necessary to fulfil its mandate.

In situations where engagement with vulnerable persons is necessary, volunteers are explicitly instructed to adhere to the **principle of necessity and minimization**. This principle emphasizes conducting interactions only when essential and minimizing any potential harm to the individuals involved. Furthermore, volunteers are directed to adopt a **victim- or survivor-centered approach**, placing the well-being, dignity, and rights of the vulnerable persons at the forefront of their interactions. By prioritizing the needs and perspectives of those they engage with, volunteers ensure that their actions are conducted with empathy, respect, and sensitivity, promoting a supportive and empowering environment for all participants.

Recommendation: Foundation should persist in expanding its network of contacts with centres that provide psychological support and define coping measures within its team, and identify services and professionals who can provide support when necessary.

8 The Foundation's Method of Collecting Information

The primary goal of the Foundation is to ensure the quality and reliability of the information provided while safeguarding the best interests of the individuals giving their accounts. For these purposes, we prioritize both the appropriate assistance provided by our volunteers and the suitability of the questionnaire form.

The Foundation operates under the assumption that the majority of individuals will independently complete the form in a serene and focused manner, choosing a time and place where they feel secure. Our volunteers are available to provide assistance in filling out the form when requested by the individuals possessing the pertinent information. In such cases, our volunteers will offer guidance on how to add information to the form and how to submit the completed form.

We anticipate that most individuals will take the initiative to complete the form on their own when they are ready. However, if they require additional assistance, our volunteers will be readily available to provide support during the initial contact and, if needed, in subsequent interactions.

During the initial training, all volunteers are provided a checklist (Do and Don't lists) for all meetings with persons giving an account to ensure their compliance and that they cover all the necessary points. This checklist is aimed at helping volunteers to stay organized and attentive during the interactions, ensuring that important aspects are addressed and that the person's experience is respected and thoroughly documented.

At the preparation stage, our volunteers take the following steps:

1. They familiarize themselves with the purpose and objectives of the Project.
2. They understand the specific roles and responsibilities assigned to them.
3. They acquire necessary training and knowledge related to their tasks.
4. They ensure they have the required tools and resources for their assignments.
5. They clarify any doubts or seek guidance from their team members.

6. They review the guidelines and protocols to ensure adherence to best practices.
7. They establish communication channels with the person willing to give an account.

When assisting the person giving an account, our volunteers ensure that:

1. They create a safe and supportive environment for the individual to share their experiences.
2. They respect the individual's pace and comfort level during the process. They take as much time as necessary to explain to the person in detail the purpose and framework of the process.
3. They maintain confidentiality and safeguard the privacy of the information shared.
4. They introduce the team, the organisation and its mandate, they explain how the app works.
5. They provide necessary information about the documentation process, its purpose and potential use of the information collected.
6. They emphasize the utmost importance of providing an accurate account. They explain to the person that they are free to answer or decline any questions, and if there is uncertainty or lack of knowledge regarding a specific inquiry, they can simply acknowledge it. They make it clear that the person has the right to terminate the account at any point if they wish to do so.
7. They offer guidance and support, should the individual require emotional assistance.
8. They are patient, and ensure that the person understands all of the above and seek informed consent regarding his or her voluntary participation in the process.

The Project Sunflowers's **questionnaire** includes the following parts:

- I. **PART A - Personal details:** name, surname, patronymic/paternal name, nationality, date of birth, place of birth, sex, address of last residence, address of intended stay, street, house number, flat number, postcode, city, country, phone number, e-mail address, social media profile, information on persons who can facilitate contact,
- II. **PART B - Crime details:** event, time period of the event, category of event, location, detailed description of the site, description of event, attachments – evidence in possession, showing the event (photos, films, etc.); additional witness to the event, perpetrators of event (name, surname, additional information to help identify)

- III. **PART C - Damage details:** damage suffered, time period of damage, category of damage, location, description of damage, description of event causing damage, attachments – evidence in possession, showing the event (photos, films, etc.); damage perpetrators (name, surname, additional information to help identify);
- IV. **PART D - Additional statements:**
- a) If you have given the information you submitted to other law enforcement agencies (or similar institutions), you can list it here. The information may be useful to law enforcement agencies in their mutual coordination regarding the listed crimes and damages.
 - b) I have read the regulations and privacy policy and I accept their provisions.
 - c) I declare that I have provided true information.
 - d) I consent to the processing of my personal data, including the special category of data submitted by me in this form, by the Foundation Sunflowers, based in Warsaw, for the purpose of collecting information about evidence and victims of crimes committed in Ukraine as of 24 February 2022 and providing it to the authorized authorities. I know that I can withdraw my consent at any time.
 - e) GDPR information clause.

9 Storing and Safeguarding

Our application has been developed by a company with extensive experience in creating applications for the secure collection of sensitive data, including a proven track record in whistleblower protection. It is being securely stored in the cloud provided by globally recognised server provider and it incorporates diverse features designed to enhance the security and integrity of the stored data.

The Foundation guarantees **the preservation of the integrity** of every item and piece of information collected from the moment it is obtained until it is handed over to the competent investigative authorities.

Throughout this period, the Foundation takes all necessary measures to **protect the items and information from any damage, loss, alteration, or tampering.**

The Foundation ensures compliance with applicable legislation regarding the **protection of personal data**, prioritizing the privacy and confidentiality of all collected information. The comprehensive measures in place showcase adherence to best practices and the utmost professional standards in data protection. These encompass various strategies such as isolating data from contact particulars and segregating statements from incident and damage information. Encryption protocols are deployed for data both at rest and in transit,

complemented by ongoing staff training. Rigorous audit trails ensure traceability and responsibility for individuals accessing infrastructure and applications. Access control for IT administrators is tightly regulated, supplemented by automated anomaly alerts. Cloud providers furnish advanced defences against DoS and DDoS attacks, bolstered by geographic restrictions and strict access protocols for individual infrastructure elements. Roles are distinctly separated, databases physically segmented when necessary, and security measures aligned with OWASP recommendations. External auditors conduct security assessments, while continuous automatic monitoring oversees both infrastructure and applications. Assurances include 99.999999999% data durability via AWS S3 services, a high infrastructure availability rate of 99.99% through duplicated system components, seamless transitions to backup servers upon failure, and secure storage of automatic security copies in a protected location.

To maintain **the utmost transparency and accountability**, the Foundation meticulously maintains a comprehensive chain of custody for every piece of information collected. This includes detailed documentation of the information's whereabouts and the **identification of every individual who accessed and handled it**, from the moment of reception or creation until it is handed over to an investigating authority.

10 Annexes

1. Declaration of voluntary submission
2. Privacy policy
3. Terms of use
4. Regulations of Procedure for the Transmission of Information within the Project Sunflowers

11 Recommendations Summary

General principles: The Foundation Sunflowers should carefully consider the importance of implementing a standardized documentation procedure that incorporates all these guidelines. Currently, the volunteers are undergoing training in these procedures. It should be considered to develop a knowledge base, also in documented form, to facilitate knowledge sharing and enhance procedural transparency

Do no harm: Given the expanding nature of the database, it is of utmost importance to undertake a thorough reassessment of potential risks and perpetually monitor actions that warrant attention, amenable to modification to better align with the "do no harm" principle.

Among the actions that necessitate focus in adherence to the "do no harm" principle, emphasis should be placed on the robustness of the referral support system and meticulous care for vulnerable individuals.

Additionally, the stability and security of the database demand heightened scrutiny to ensure the protection of sensitive information and to uphold the integrity of the Foundation's mission in safeguarding the well-being and rights of all participants involved.

Objectivity, impartiality and independence: These principles should be incorporated into the documented standards, upheld during all activities, and consistently reminded to all volunteers.

Accountability and legality: The Foundation should maintain a detailed record of methods and procedures for preserving and collecting information.

Professionalism and respect: These principles should be incorporated into the documented standards, upheld during all activities, and consistently reminded to all volunteers.

Confidentiality: the Foundation should ensure that all team members, intermediaries and interpreters are trained in and comply with confidentiality requirements and information protection protocols. The GDPR documentation should be regularly implemented and each new Project's member should be trained on GDPR compliance procedures.

The Foundation should prioritize the implementation of access monitoring to track and record user logins, including information on who logged on, when they logged on, and what resources they accessed. This measure will enhance the security and accountability of the organization's information systems.

At a later stage, particularly when sharing information with enforcement authorities, the Foundation should consider the development of a dedicated module for managing and controlling access privileges. Additionally, the implementation of Multi-Factor Authentication (MFA) to verify the identity of users accessing the system should be explored. It's important to note that these advanced security measures may not be required at the initial stage of information request, where volunteer verification of individual identity is deemed sufficient. However, as the Foundation's operations expand and involve sensitive data sharing, enhancing security with MFA and access control becomes increasingly important.

Vicarious trauma: The Foundation should maintain an ongoing commitment to monitoring vicarious trauma-related concerns and proactively address requests for additional training or assistance in locating support resources, such as supervision.

Furthermore, the Foundation should persist in expanding its network of contacts with centres that provide psychological support, with a particular emphasis on the countries where our volunteers and contributors are situated. Foundation should define coping measures within its team, and identify services and professionals who can provide support when necessary.

Vulnerable persons: Foundation should persist in expanding its network of contacts with centres that provide psychological support and define coping measures within its team, and identify services and professionals who can provide support when necessary.

Declaration of voluntary submission



You are about to open a form in which you can report an event that could be considered as international crime or other serious violation of human rights, and/or harm you have suffered in regard to the war in Ukraine. The submission of information is voluntary. In order to ensure that the form is completed correctly, instructions have been developed in the form of interactive tools, visible when filling in the form. At each stage of the information collection, the person who filled in the form has access to the information, able to add or delete it securely.

The information collected is stored in a secure database. The information, together with the data of the persons submitting it, will then be made available only to international and national authorities empowered to prosecute the crimes, in particular to the Prosecutor of the International Criminal Court, and to the national prosecutors' offices of the countries investigating the crimes. The information will also be available for use by international tribunals and national courts in proceedings relating to crimes committed in Ukraine as of 24 February 2022, and in possible reparation proceedings to compensate for the damage caused.

The form uses an autosave option. It is also possible to save the form without submitting it (draft version). Therefore, the collection of information starts as soon as you start filling in the form. Each draft version of the form can be completed within a further six months. After this period has expired without success, your data will be erased definitively from the database.

At any stage of the collection of information, any person may complete their form or withdraw it. In order to do so, you must - according to your intention - select the relevant draft form to complete it, or withdraw the form you have submitted (to do so, you must follow the separate instructions you will receive in your email as a response to the initiation of the withdrawal procedure).

Any person who wishes to share their war story can be assured that any information they provide will be securely stored and used to preserve historical truth even if the information is not used in criminal proceedings.

The administrator of the data is the Foundation Sunflowers with its registered office in Warsaw (01-204), 5/51 Siedmiogrodzka St. Your personal data will be processed in order to enable you to provide the Foundation with information about crimes in Ukraine. You have the right to access your personal data, rectification, erasure, limitation of processing and data portability and to make a complaint to a supervisory authority. For more information about the processing of your personal data, please see [the Privacy Policy](#).

By proceeding to complete the form you accept the terms and conditions found at the link: <https://forms.projectsunflowers.org/en/assets/documents/terms-of-service-en.pdf>.

Cancel

I understand and wish to complete the submission



Privacy Policy
www.projectsunflowers.org
valid as of 3 November 2023

This Privacy Policy provides information regarding **the processing of personal data by Foundation Sunflowers, based in Warsaw, Poland, in accordance with Articles 13 and 14** of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR").

The Privacy Policy applies to the processing of data of individuals who use www.projectsunflowers.org (the "**Service**"), interact with the Foundation, including through the use of social media, participation in webinars and trainings of the Foundation (the "**User**") or whose data has been provided to the Foundation by third parties.

1. ADMINISTRATOR

1. The administrator of the personal data of the website's users available at www.projectsunflowers.org is **the Foundation Sunflowers with its registered office in Warsaw, Poland** (Siedmiogrodzka street no. 5/51, 01-204 Warsaw), entered in the Register of Associations, Other Social and Professional Organisations, Foundations and Independent Public Health Care Units of the National Court Register kept by the District Court for the Capital City of Warsaw in Warsaw, XIII Commercial Division under KRS no.: 0001019393, NIP: 5273044660 ("**Administrator**").
2. Contact with the Administrator is possible by means of postal correspondence to the above-mentioned address and via e-mail address: contact@projectsunflowers.org

2. SERVICE AND SUNFLOWERS PROJECT

- 2.1. The Service was established in order to collect information about evidence and victims of crimes committed in Ukraine as of 24 February 2022 and to provide this data to authorised national and international law enforcement and justice authorities (the "**Project**").
- 2.2. The Administrator collects the aforementioned information through a dedicated application form available on the Service (the "**Form**").
- 2.3. The data comes from users of the Website who submit the Form to the Administrator. In the Form, the User may provide both his/her personal data and the personal data of third parties.

3. PURPOSES AND GROUNDS FOR DATA PROCESSING

- 3.1. The Administrator processes the following personal data

3.1.1. Users:

- 3.1.1.1. **who have requested to be contacted by the Foundation in order to enable it to provide them with information about crimes** - the legal basis is consent (Article 6(1)(a) GDPR). The administrator processes the following data: name, surname, telephone number, email address, language, country of residence.
- 3.1.1.2. **who have registered an account with the Project** - the legal basis is the necessity of the processing to perform the concluded contract with the personal data subject (Article 6(1)(b) GDPR). The Administrator processes the following data: surname, e-mail address.
- 3.1.1.3. **who started to fill in or sent the Form to the Administrator for the purpose of collecting information about evidence and victims due to crimes committed in Ukraine as of 24 February 2022 and forwarding it to authorised authorities** - the legal basis is the necessity of processing for the performance of the concluded contract with the personal data subject (Art. 6(1)(b) GDPR) and the user's consent to the processing of special category personal data (Article 6(1)(a) in conjunction with Article 9(2)(a) GDPR) and data provided on an optional basis (Article 6(1)(a) GDPR).
- 3.1.1.4. **contacting the Administrator**, in order to handle and respond to enquiries addressed by Users to the Administrator - the legal basis for processing is the consent of the data subject (Article 6(1)(a) GDPR). The Administrator processes the User's personal data provided voluntarily in the content of the message;
- 3.1.1.5. **those interacting with the Administrator via social network profiles**, in order to administer the Administrator's profile on social networks, by responding to messages, comments and reactions, as well as for statistical and advertising purposes carried out by means of the tools provided by these social networks - on the basis of the Administrator's legitimate interest (Article 6(1)(f) GDPR), which is communication with social network users and provision of informative content about the Administrator and its activities. The Administrator processes User data publicly available on the social network, such as name, surname, image and those provided voluntarily in the content of a message or comment.
- 3.1.1.6. **enrolled in a webinar or training organised by the Administrator** in order to enable the User to participate in the event - the legal basis for processing is the User's consent expressed by signing up for the event (Article 6(1)(a) GDPR). The Administrator processes User data such as name, surname, email address.
- 3.1.1.7. **subscribed to the newsletter** in order to receive information concerning the Administrator by electronic mail (e-mail) - the legal basis for processing is the Administrator's legitimate interest in marketing its services (Article 6(1)(f) GDPR) in connection with the User's consent expressed in accordance with the Act on Providing Services by Electronic Mail and the Telecommunications Law. The Administrator processes the User's personal data entered by the User in the contact form, i.e. name, surname and e-mail address.

- 3.1.2. **The persons indicated by the Users within the Project via the Form** - in order to realise the legitimate interest of the Administrator and the User who provided the data of these persons (Article 6(1)(f) GDPR), consisting in the execution of the Project by the Administrator and for the purposes of evidentiary proceedings concerning the event referred to in the form sent by the User.

- 3.2. In addition, the personal data of the persons whose data the Administrator processes may also be processed by the Administrator for the purposes of possible establishment, investigation or defence against claims. The legal basis for the processing is the legitimate interest of the Administrator (Article 6(1)(f) GDPR) to protect one's rights or for the Administrator to assert them.

4. WHERE DOES THE DATA WE PROCESS COME FROM?

- 4.1. The data of Users who browse the Portal, fill in and send the Form within the Project, subscribe to a webinar or newsletter or otherwise contact the Administrator come directly from the person concerned.
- 4.2. Data of persons indicated in the Form by Users, including witnesses of reported incidents or those who can facilitate contact with the User, are provided to the Administrator by Users within the Form sent to the Administrator. The data that the Administrator processes as a result of receiving it from Users includes name, surname, email address, telephone number, social media profile. The Administrator does not collect or require this data itself.

5. VOLUNTARINESS OF DATA PROVISION AND CONSENT

The provision of data by the User is voluntary, but necessary for the purpose for which they are provided, i.e. the collection of information about events in Ukraine, for the purposes of communication, including via social media, or participation in an event organised by the Administrator. Without their provision, it will not be possible to achieve the particular purpose the User wishes to achieve, i.e. for the Administrator to respond or for the User to participate in an event.

6. PERIOD OF PERSONAL DATA PROCESSING

- 6.1. The Administrator will process personal data for the following period of time:
 - 6.1.1. personal data processed on the basis of the User's consent - until the consent is withdrawn; at the same time, in the case of Users who have declared their wish to contact the Foundation in order to enable them to provide information about the crimes, the data shall be processed for no longer than 1 month from the moment of declaring the wish to contact;
 - 6.1.2. the personal data of Users who have registered an account and the data provided within the Form - for the duration of the contract for the provision of electronic services between the User and the Administrator;
 - 6.1.3. personal data of persons whose data was provided by the User in the Form, which is processed on the basis of the legitimate interest of the Administrator - for the entire duration of such interest, but no longer than until the User or the person concerned objects to such processing; in the case of data provided in the Form, which was saved and not sent to the Administrator - the data will be processed no longer than 6 months from the moment of saving the Form;
 - 6.1.4. personal data processed within the framework of social networking sites - for the duration of the Administrator's legitimate interest (but no longer than until an objection is made to such processing), the functioning of a given social networking service or the deletion of the User's account in this service.
 - 6.1.5. personal data of persons given for the purpose of receiving the newsletter - for as long as there is a legitimate interest of the Administrator consisting in marketing its own services, no longer than until an objection is raised or consent is withdrawn on the basis of the Act on the provision of electronic services or Telecommunications Law;
 - 6.1.6. personal data of persons enrolled in webinars or trainings - until the webinar or training is over.
- 6.2. The period of personal data processing may be extended by the Administrator until the statute of limitations for potential claims related to the data processing.

7. RECIPIENTS OF DATA

- 7.1. The personal data of Users who submitted the Form and the personal data of persons indicated in the Form as witnesses or contact persons shall be made available by the Administrator at the request of competent national and international law enforcement and justice authorities pursuant to applicable laws.
- 7.2. Recipients of personal data of persons whose data is processed by the Administrator are entities cooperating with the Administrator in the performance of their duties, providers of IT, hosting, e-mail, accounting, legal services, providers of social networks, providers of real-time communication platforms, providers of newsletter tools.
- 7.3. The third parties referred to above are obliged under the relevant agreements to use the data entrusted to them only for the purpose indicated by the Administrator. These entities are also obliged to adequately secure the personal data and keep it confidential.

8. SECURITY OF PERSONAL DATA

- 8.1. **In order to take care of the security of your personal data and other information provided to us, in particular through the Form, we have implemented appropriate technical and organisational measures. We take a number of measures to ensure that the processing of your data complies with the GDPR and other data protection legislation.**
- 8.2. In selecting the safeguards to be applied, we have taken into account, among other things, the nature of the personal data you provide to us, as well as the risk of a breach of your rights in the event of a breach of the protection of your personal data and its likelihood. All the solutions we use are designed to protect your rights.
- 8.3. Furthermore, through the Service, including the Form, we only collect the data necessary for the purposes set out in the Privacy Policy.
- 8.4. Only necessary and authorised persons also have access to the processing of personal data. They have also been obliged to maintain confidentiality or are covered by the obligation of professional secrecy.
- 8.5. Personal data of Users and third parties provided by Users are not subject to automated decision-making, including profiling.

9. RIGHTS OF DATA SUBJECTS

- 9.1. Any person whose personal data is processed by the Controller has the right to:
 - 9.1.1. access to the data and to obtain a copy of the data,
 - 9.1.2. rectification, erasure, restriction of processing, data portability,
 - 9.1.3. **if personal data are processed on the basis of consent, the data subject has the right to withdraw it at any time. The withdrawal of consent does not affect the lawfulness of processing on the basis of consent until the consent is withdrawn.**
 - 9.1.4. **to object at any time to the processing of his/her data for direct marketing purposes, including profiling, where the processing is carried out in relation to the legitimate interest of the Controller.**
 - 9.1.5. **object at any time to the processing of his/her data for reasons related to his/her particular situation in cases where the legal basis of the processing is the legitimate interest of the Controller.**
 - 9.1.6. to lodge a complaint with the President of the Office for the Protection of Personal Data if he/she considers that the processing of his/her personal data violates the provisions of the GDPR.
- 9.2. To exercise any of the above rights, please send an email to contact@projectsunflowers.org
- 9.3. With regard to co-mediated personal data processed through social networking services, the User may exercise his or her rights vis-à-vis the operator of the social networking service in accordance with the rules laid down by the latter:
 - a. Facebook: <https://www.facebook.com/privacy/explanation>
 - b. LinkedIn: <https://pl.linkedin.com/legal/privacy-policy?src=li-other&veh=www.linkedin.com%7Cli-other#other>
 - c. Instagram: <https://privacycenter.instagram.com/policy>.

10. TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

- 10.1. The Administrator transfers personal data to third countries, outside the European Economic Area, i.e. to the United States, only for the purpose for which they were made available to the following entities, due to the international nature of these entities.
- 10.2. Data of users interacting with the Administrator via social media is transferred outside the EEA, to:
 - 10.2.1. Meta Platforms Inc. based in California, USA - the entity that is responsible for the Administrator's facebook.com fan page. Information on privacy standards: <https://www.facebook.com/privacy/explanation>
Meta Platforms Inc has stated that it has implemented standard contractual clauses, which you can read about here: <https://www.facebook.com/business/help/336550838147603> and <https://privacycenter.instagram.com/policy>.
Meta Platforms Inc stated that it has implemented standard contractual clauses, which you can read about here: <https://www.facebook.com/business/help/336550838147603> and https://help.instagram.com/272603474673152/?helpref=uf_share.
The transfer is based on the European Commission's Implementing Decision of 10 July 2023 on the Adequacy of Personal Data Protection under the EU-US Data Privacy Framework and the listing of Meta Platforms Inc. as a participant in the Data Privacy Framework.
 - 10.2.2. LinkedIn Corporation, based in California, USA - the entity that is responsible for the operation of the Administrator's linkedin.co.uk account. Information on privacy standards, including the implementation of standard contractual clauses: <https://www.linkedin.com/help/linkedin/answer/62533>
- 10.3. Data of users enrolled in webinars and trainings organised by the Administrator is transferred outside the EEA to Zoom Video Communications Inc. based in San Jose, USA - a provider of a real-time communication platform. The provider has implemented standard contractual clauses, which you can read about here: <https://explore.zoom.us/pl/gdpr/>.

11. SOCIAL MEDIA CO-ADMINISTRATION

- 11.1. In connection with the Administrator's operation of:
 - 11.1.1. a fan page on Facebook at: <https://facebook.com/theprojectsunflowers/>, and a Administrator's profile on Instagram at: <https://www.instagram.com/project.sunflowers/>, the Administrator is the joint data controller of the Users' data with the provider of the service, i.e., Meta Platforms Ireland Limited with its registered office in Dublin (Ireland), address: 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, D02X525, Ireland
 - 11.1.2. the Administrator's profile on LinkedIn at <https://linkedin.com/company/projectsunflowers/>, the Administrator is the joint data controller of the Users' data with the service provider, i.e., LinkedIn Ireland Unlimited Company with its registered office in Dublin (Ireland), address: Wilton Place, Dublin 2, Ireland, ("Joint Administrators").
- 11.2. The co-administration includes the aggregate analysis of data, the purpose of which is to display statistics on the activity of the Users of the fan page on the service and advertising activities through the tools available there.
- 11.3. For more information about Facebook and LinkedIn and the arrangements between the Joint Administrators (including their respective responsibilities), please see:
 - 11.3.1. the Facebook privacy policy at: <https://www.facebook.com/privacy/explanation> and https://www.facebook.com/legal/terms/page_controller_addendum
 - 11.3.2. the LinkedIn privacy policy at: <https://pl.linkedin.com/legal/privacy-policy?src=li-other&veh=www.linkedin.com%7Cli-other#other>
 - 11.3.3. the Instagram privacy policy at: <https://privacycenter.instagram.com/policy>

12. SERVER LOGS

- 12.1. The usage of the Service is linked to the sending of requests to the server on which the Service is stored. Each query sent to the server is recorded in server logs, which are saved and stored on the Service.
- 12.2. The logs include, but are not limited to, the User's IP address, the date and time of the server, information about the Internet browser and the operating system the User is using.
- 12.3. The data recorded in the Server logs are not associated with particular users using the Service and they are not used by the Administrator to identify the Users.
- 12.4. Server logs are only auxiliary material used for administering the Service and their content is not disclosed to anyone except persons authorized to administer the Service.

13. COOKIES

- 13.1. We use various cookies listed on the cookie banner, which may contain personal data from your browser (such as your IP address, unique cookie identifier; unique device identifier and device type; domain, browser type and language, operating system and system settings; country and time zone; previously visited websites; information about your interaction with the Service; and access times and referring URLs).
- 13.2. We use cookies on the Website for the purposes necessary for its operation and, with your consent, for analytical and advertising purposes.
- 13.3. The Service does not collect any information by automatic means, except for the information contained in cookies. Cookies necessary for the proper functioning of the Service, which are always active and cannot be deactivated. As for other cookies, we may collect them if the User agrees by using the cookie banner.
- 13.4. Refusing to accept cookies other than those necessary for the Service may result in related functions not being available.
- 13.5. You can change your cookie settings at any time. To do so, please use the icon shown in the bottom left-hand corner of the Service, which allows you to access your cookie settings.
- 13.6. Third parties may also collect information through our website by means of cookies, third-party plug-ins and widgets. These third parties collect data directly from your browser and the processing of this data is subject to their privacy policy.
- 13.7. Information on cookies, their types, storage periods and providers can be found in the cookie banner.

14. CONTACT

The Administrator shall provide the persons whose data he processes with the possibility to contact him in all matters concerning data protection via e-mail at the following address: contact@projectsunflowers.org



TERMS OF USE

www.projectsunflowers.org

Foundation Sunflowers based in Warsaw

§ 1. Definitions

The terms used in these Regulations shall be understood as follows:

1. **Service Provider** - Foundation Sunflowers with its registered office in Warsaw, at ul. Siedmiogrodzka 5/51, 01-204 Warsaw, entered in the Register of associations, other social and professional organisations, foundations and independent public health care institutions of the National Court Register kept by the District Court for the Capital City of Warsaw in Warsaw, XII Economic Division of the National Court Register, under the KRS number 0001019393, NIP 5273044660, e-mail: contact@projectsunflowers.org ;
2. **Service** - the website available at <https://projectsunflowers.org> ;
3. **User** - natural person over 18 years of age with full legal capacity, using the Newsletter or concluding an agreement to participate in a Webinar;
4. **Newsletter** - information of a commercial nature concerning the Service Provider's activities and events organised by the Service Provider, including fund-raisers and donation opportunities, as well as Webinars, sent by email, at the request of the User;
5. **Webinar** - online training conducted by the Service Provider for Users live (real-time transmission) at a place and time specified by the Service Provider within the platform indicated by the Service Provider;
6. **Regulations** - these regulations;
7. **Services** - services provided electronically on the Service by the Service Provider.

§ 2. Regulations

1. The Regulations define in particular:
 - a. the scope and conditions for the provision of services provided electronically on the Service,
 - b. the conditions for entering into and termination of the agreement for the provision of Services,
 - c. technical requirements necessary to use the Services,
 - d. principles of submitting and investigating complaints,
 - e. principles of the Service Provider's liability.
2. Before using the Services, the User is obliged to read the Regulations and the [Privacy Policy](#). Beginning to use the Services implies acceptance of the Regulations.
3. Regulations are made available free of charge through the Service, in a manner that allows obtaining, reproducing and recording the content of the regulations by means of teleinformatic system, which is used by the Service Recipient.
4. The Regulations are the regulations referred to in Article 8 of the Act of 18 July 2002 on provision of services by electronic means.

§ 3. Technical conditions

1. The minimum technical requirements to use the Services are:
 - a. use of a device that communicates with the Internet,
 - b. an installed and up-to-date operating system on the device,
 - c. an updated and current web browser,
 - d. a stable Internet connection,
 - e. an active e-mail account,
2. A speaker/headset is also required in order to participate in the Webinar, and the use of tools from an external provider and the registration of an account by the User may be required.
3. The Service Provider is not a provider of data transmission or telecommunications services. Any costs related to data transmission services or telecommunication services required to use the Newsletter and Webinars shall be borne solely by the User on the basis of separate agreements concluded by the User with providers of the aforementioned services.
4. The Service Provider declares that due to the public nature of the Internet, the conclusion of the agreement and use of the Newsletter or participation in the Webinar may involve the risk of obtaining, appropriating or modifying the User's data by unauthorised persons. Consequently, the User should use appropriate technical measures to minimise the aforementioned risks, including anti-virus or identity protection software.

§ 4. Services provided electronically

1. The Services provided on the Service include:
 - a. the sending of a Newsletter by the Service Provider at times selected by the Service Provider to the User's e-mail address;
 - b. a contact form through which the User may contact the Service Provider on matters of his/her choice ("Form");
 - c. to enable Users to participate in Webinars.
2. As part of the Service, the Service Provider also enables the submission of notifications to the Project Sunflowers. The requirements for submitting notifications are governed by separate [regulations](#).
3. The use of the Services is free of charge.
4. Subject to other express provisions in the Regulations, the Services shall be provided 24 (twenty-four) hours a day, 7 (seven) days a week, at the request of the User, unless otherwise specified in the Regulations.
5. The place where the Services are provided is the territory of the Republic of Poland.

§ 5. Newsletter

1. The Service Provider shall make it possible for the User to conclude an agreement for the provision of digital content in the form of a Newsletter in exchange for the User providing their personal data.
2. The Newsletter service shall be free of charge. In order to receive the Newsletter, the User is not obliged to provide any services other than providing personal data in the form of name and e-mail address.
3. The Newsletter contains information of a commercial nature concerning the activities of the Service Provider and events organised by the Service Provider, including Webinars.
4. The Newsletter may contain links redirecting to websites other than those of the Service Provider. In this case, the User is obliged to comply with the regulations applicable to these websites.
5. The Newsletter is sent by the Service Provider via e-mail to the e-mail address indicated by the User, upon request.
6. The Newsletter service is provided for an indefinite period of time, on a continuous basis.
7. The Newsletter need not and is not delivered to Users on a regular basis. The time of delivery of the Newsletter to Users shall be decided by the Service Provider.
8. In order to conclude a contract for the provision of digital content within the Newsletter (i.e. signing up for the Newsletter), the User:

- a. fills in the dedicated Newsletter sign-up form on the Service, providing his/her personal data, i.e. name, surname, email address, and sends it to the Service Provider using the "Subscribe" button or the same, and
- b. confirms the sign-up and the email address by means of the activation link contained in the message sent to the User at the email address indicated (double opt-in mechanism).
9. The contract for provision of digital content (Newsletter subscription) shall be concluded upon confirmation of the subscription.
10. Signing up for the Newsletter shall signify acceptance of the Regulations.
11. Subscribing to the Newsletter shall be equivalent to consent to receive commercial information concerning the Service Provider, pursuant to Article 10 of 18 July 2002 on the provision of electronic services.
12. The User may subscribe to the Newsletter 24 (twenty-four) hours a day, 7 (seven) days a week.
13. The Newsletter Contract shall be concluded in Polish or English, the choice of which shall be made by the User.
14. The place of provision of the Newsletter service shall be the territory of the Republic of Poland.
15. The User may terminate the agreement for provision of digital content within the Newsletter at any time and without stating a reason, with immediate effect.
16. In order to terminate the Agreement, the User should:
 - a. click on the "Unsubscribe" link or the equivalent, visible in the footer of each Newsletter email; or
 - b. send a message requesting unsubscription from the Newsletter to the Service Provider's email address: contact@projectsunflowers.org.
17. The Service Provider may terminate the Newsletter service agreement with immediate effect for valid reasons, i.e. in the event of:
 - a. violation by the User of provisions of generally applicable law or the Regulations, including § 7 section 2 of the Regulations,
 - b. provision by the User of erroneous or false data (which results in the impossibility of proper implementation of the Service) or provision of third party data,
 - c. when the User undertakes actions which disrupt the Signing up for the Newsletter shall be considered as consent to receive commercial information concerning the Service Provider, pursuant to Article 10 of 18 July 2002 on operation of the Website or interfere with the Newsletter service for other Users,
 - d. when the User uses the Newsletter service for sending illegal content or violates or attempts to violate the technical protection of the Website or Newsletter service,
 - e. in case of inactivity of the User for a period of one year, including non-opening of messages by the User, which does not require prior notification of the User by the Service Provider.
18. The Service Provider may terminate the Newsletter service agreement at any time with 14 days' notice, of which the User will be informed by email.

§ 6. Webinar

1. The Service Provider enables the User to participate in Webinars in exchange for the Users providing their personal data.
2. Participation in the Webinar is free of charge. In order to participate in the Webinar, the User is not obliged to provide any services other than providing personal data in the form of name and e-mail address.
3. The information about the Webinar, including the date, duration, subject matter, language in which the Webinar is conducted, programme and technical conditions are specified each time in the information about the Webinar. The Service Provider may provide simultaneous translation at its discretion, depending on the capacities.
4. Webinars are not and do not have to be organised periodically. It is at the Service Provider's discretion to organise a particular Webinar, including its running time and subject matter.
5. Participation in Webinars is possible in real time (live transmission), at the time specified by the Service Provider and through the tools indicated by the Service Provider in the Webinar information.
6. In order to participate in the Webinar, the User fills in the dedicated form for Webinar enrolment, providing his/her personal data, i.e. name, surname, email address, and sends it to the Service Provider by means of the "Save" button or an identical one.
7. When signing up for the Webinar, the User may agree to receive the Newsletter (optional).
8. Enrolment in the Webinar implies acceptance of the Regulations.
9. The contract for participation in the Webinar is concluded as soon as the enrolment is made in accordance with point 6 above.
10. The User may only sign up for a Webinar if the Service Provider informs the User about the planned Webinar, prior to the Webinar.
11. The Webinar participation agreement is concluded in Polish or in another language provided by the Service Provider, the choice of which is made by the User.
12. The place of Webinar service provision is the territory of the Republic of Poland.
13. The Service Provider shall be entitled to use any tool for Webinar and to change it at any time. In the case of some tools, the User may be required to take additional actions, such as registering an account with the tool in question.
14. Details related to the conduct of the Webinar will be made available no later than 2 days before the date of the Webinar. In the event of a change in the tool used by the Service Provider, the period referred to in the preceding sentence may be shortened.
15. The Service Provider shall be entitled to cancel or reschedule the Webinar due to force majeure, understood in particular as: the indisposition of the persons conducting the Webinar, the lack or poor quality of the Internet connection or a malfunction of the platform making it impossible to conduct the Webinar. In such a case, the User shall not be entitled to claim against the Service Provider.

§ 7. Contact form

1. Through the Form, the User may contact the Service Provider for the purpose of his/her choice.
2. The User may use the Form 24 (twenty-four) hours a day, 7 (seven) days a week.
3. The contract for the provision of the Service is concluded as soon as the User enters the relevant data indicated on the Site and sends it to the Service Provider using the "Send message" button or similar.
4. The Sales Form is not a continuous service. As soon as the data is submitted to the Service Provider, the contract is fulfilled.

§ 8. Withdrawal from the Contract

1. The User may withdraw from the Newsletter or Webinar contract without giving any reason, within 14 (fourteen) days from the date of its conclusion.
2. Withdrawal from the Newsletter Contract shall mean cancellation of the Newsletter as of the date of withdrawal, and withdrawal from the Webinar participation contract shall mean unsubscribing the User from the list of participants.
3. In order to unsubscribe, the User should:
 - a. click on the link "Unsubscribe" or the same, visible in the footer of each email sent within the Newsletter; (applicable only for the Newsletter) or
 - b. send a message requesting unsubscription from the Newsletter or removal from the list of Webinar participants to the Provider's email address: contact@projectsunflowers.org.

§ 9. User Obligations

1. The User is obliged to use the Service and the services in a manner consistent with the law and the Regulations, including:
 - a. use the Services in a manner that does not infringe the rights of third parties, good morals or the law,
 - b. not to post misleading or unlawful content on the Services,
 - c. use the Services and Service in a manner that does not interfere with their functioning,
 - d. respect the Service Provider's rights, including copyright and intellectual property rights, to the Service and material published on the Service and on the Services,
 - e. to refrain from transmitting data, including personal data of third parties, without an appropriate legal basis, including the consent of such parties.
2. Within the Services, it is prohibited for the User to provide content of an unlawful nature. In the event that the Service Provider receives an official notice or credible knowledge of the unlawful nature of the data stored or provided by the User, the Service Provider may prevent access to such data and/or terminate the contract with the User with immediate effect.

§ 10. Service Provider's liability

1. The Service Provider shall be indemnified against any liability for claims relating to the use of the Services or the Service as a result of non-compliance with the Regulations.
2. To the extent permitted by law, the Service Provider shall not be liable for:
 - a. disruptions in the operation or impediments to access to the Service and/or the Services caused by circumstances for which the Service Provider is not responsible, including the actions of telecommunications operators;
 - b. lack of possibility or difficulties in using the Service and/or the Services due to failure to meet the technical requirements specified in the Regulations,
 - c. the consequences of vis maior,
 - d. the consequences of the actions of third parties, including the User, for which the Service Provider is not responsible,
 - e. the consequences of the User's provision of untrue, incomplete or incorrect data when using the Services, for non-delivery of the Newsletter or e-mail notifications regarding the Webinar for other reasons attributable to the User, e.g. an overflowing mailbox,
 - f. third party data provided by the User in the Services,
 - g. for the User's assimilation of knowledge and information communicated during the Webinar or sent as part of the Newsletter, or for any claim by the User that the level of content was inadequate or did not meet his or her expectations.

§ 11. Non-compliance with the contract. Complaints

1. The Service Provider shall be liable to the User for the conformity of the digital content provided within the Newsletter or Webinar with the Contract, in accordance with Chapter 5b of the Consumer Rights Act (Articles 43a-43g).
2. The Service Provider is liable for non-conformity with the Contract that existed at the time of delivery of the digital content and became apparent within two years of that time. A non-conformity that has become apparent within one year of the delivery of the digital content shall be presumed to have existed at the time of delivery.
3. If the digital content is not in conformity with the Contract, the User may request that the digital content be brought into conformity with the Contract by means of a complaint.
4. The complaint may be addressed to the Service Provider electronically by means of a message sent to the email address: contact@projectsunflowers.org.
5. The complaint should contain at least the following information: (i) the User's e-mail address, (ii) a description of the circumstances justifying the complaint, (iii) the User's request.
6. If the complaint does not contain the data indicated in para. 5 above, the Service Provider may request the User to complete the data. If all data are not provided, the complaint cannot be considered by the Service Provider.
7. Complaints are considered within 14 (fourteen) days from the day the Service Provider receives the complaint, of which the User will be notified by e-mail to the e-mail address provided by the User.
8. If the complaint is accepted, the Service Provider shall bring the digital content into conformity with the contract within a reasonable time from the time it was informed of the lack of conformity and without undue inconvenience to the User.
9. The Service Provider may refuse to bring the digital content into conformity with the Contract if this is impossible or would require excessive costs for the Service Provider.
10. If the digital content is not in conformity with the Contract, the User may submit a declaration of withdrawal from the Contract in accordance with § 8 of the Regulations when:
 - a. bringing the digital content into conformity with the Agreement is impossible or would require excessive costs,
 - b. the Service Provider has failed to bring the digital content into conformity with the Contract,
 - c. the non-conformity of the digital content with the Contract continues even though the Service Provider has attempted to bring it into conformity with the Contract,
 - d. the non-conformity of the digital content with the Contract is so significant that it justifies the withdrawal from the Contract without the prior application of the safeguard measure specified in § 11.3 of the Regulations,
 - e. it is apparent from the Service Provider's statement or circumstances that the Service Provider will not bring the digital content into conformity with the Contract within a reasonable time or without undue inconvenience to the User.

§ 12. Personal data

1. The Service Provider is the Controller of the personal data processed in connection with the use of the Service and the Services.
2. Personal Data is processed for the purposes, to the extent and based on the grounds and principles indicated in the [Privacy Policy](#).

§ 13. Intellectual property rights

1. The Service Provider owns all rights to the Service and the digital content provided as part of the Newsletter or Webinar. Such content may constitute works within the meaning of the Act of February 4, 1994 on Copyright and Related Rights or may constitute registered trademarks and be subject to legal protection.
2. The Service Provider grants the User a non-exclusive, territorially unlimited and non-transferable license, without the right to grant sublicenses to use the digital content, for an indefinite period of time.
3. The Participant is authorized to use the digital content and other materials provided by the Service Provider exclusively for his/her own use for educational purposes only, for the entire duration of the license, in the following fields of exploitation:
 - a. storage of digital content by digital technique on the User's device,
 - b. printing of digital content available in written form.
4. It is forbidden to:
 - a. fixation, recording or other forms of copying of digital content,
 - b. displaying and making digital content available to third parties,
 - c. selling, renting or lending digital content to third parties.

§ 14. Final provisions

1. The Service Provider has the right to amend the Regulations at any time for important reasons, in particular in the event of changes in the provisions of law, changes in the terms and conditions of providing the Services, including termination of their provision, termination of operations, as well as in the event of changes in the provisions of law to the extent affecting the implementation of the provisions of the Regulations.
2. Amendments to the Regulations are effective as of the date of their publication on the Service and apply only to agreements concluded after the publication of the amendments, subject to item. 3 below.
3. Amendments to the Regulations to the extent of the Newsletter service shall become effective after 14 days from the moment of informing Users about the changes and making the amended Regulations available. If the User does not accept the changes to the Regulations, he/she should immediately, no later than within 14 days from the date of announcement of the changes, terminate the Newsletter service agreement in accordance with § 4. If the change of the digital content significantly or negatively affects the User's access to the digital content, the Service Provider will inform the User in advance on a durable medium about the type and date of the change. In such case, the User will be able to terminate the Newsletter delivery contract without notice within 30 days from the date of the change or notification of the change, if the notification was later than the change.
4. The governing law for obligations under these Regulations shall be Polish law, and disputes shall be resolved by the competent Polish common courts.
5. In matters not regulated in the Regulations, the provisions of Polish law, in particular the Act on Consumer Rights and the provisions of the Civil Code shall apply.
6. A user who is a consumer is entitled to use out-of-court ways of dealing with complaints and claims. Disputes regarding contracts concluded over the Internet can be resolved through mediation proceedings before the Provincial Inspectorates of Trade Inspection or a trial before an arbitration court at the Provincial Inspectorate of Trade Inspection. Consumers can also use other methods of out-of-court dispute resolution and, for example, submit their complaint through the EU ODR online platform, available at: <http://ec.europa.eu/consumers/odr/>.
7. The Regulations enter into force on November 6, 2023.



REGULATIONS OF PROCEDURE FOR THE TRANSMISSION OF INFORMATION WITHIN THE PROJECT SUNFLOWERS

§ 1. Service

1. The owner of the website <https://projectsunflowers.org> ("**Service**") is the Foundation Sunflowers with its registered office in Warsaw, Poland, at Siedmiogrodzka street 5/51, 01-204 Warsaw, entered in the Register of Associations, Other Social and Professional Organisations, Foundations and Independent Public Health Care Institutions of the National Court Register kept by the District Court for the Capital City of Warsaw in Warsaw, XIII Commercial Division of the National Court Register, under number KRS 0001019393, NIP 5273044660, e-mail: contact@projectsunflowers.org (the "**Foundation**").
2. The Foundation is the initiator of the Project Sunflowers, under which it makes it possible to send information to the Foundation about evidence and victims of crimes committed in Ukraine as of 24 February 2022 for transmission to authorised law enforcement and justice authorities upon their request (the "**Project**") via a dedicated form (the "**Form**") and to register and maintain an account for the submission of Forms.
3. A Service Recipient is any individual who uses the Service and the facilities necessary to provide information to the Project ("**Service Recipient**").

§ 2. Regulations

1. These Regulations ("**Regulations**") set out the terms, scope and conditions for the provision of information by the Service Recipient under the Project, including:
 - a. the terms and conditions for the conclusion and termination of the agreement for the provision of electronic services necessary for the transmission of information within the Project and the terms and conditions for their provision,
 - b. rules for filing and handling complaints,
 - c. principles of the Foundation's liability in respect of electronic services necessary for the transmission of information within the framework of the Project.
2. In order to transmit information within the Project, the Service Recipient is obliged to read the Regulations and the [Privacy Policy](#).
3. Regulations are made available free of charge through the Service, in a way that allows obtaining, reproducing and recording the content of the regulations by means of tele-information system used by the Service Recipient.

§ 3. Technical conditions

1. The minimum technical requirements for the transmission of information within the Project are:
 - a. use of a device that communicates with the Internet,
 - b. an installed and up-to-date operating system on the device,
 - c. an updated web browser,
 - d. stable internet connection,
 - e. an active e-mail account.
2. The Foundation is not a provider of data or telecommunications services. All costs related to data transmission services or telecommunication services required to use the Service and transmit information within the Project shall be borne solely by the Service Recipient on the basis of separate agreements concluded by the Service Recipient with providers of the aforementioned services.

§ 4. Submission of notifications within the Project Sunflowers

1. In order to register an account and to be able to submit a Form, the Service Recipient is required to:
 - a. declare his/her wish to be contacted by the Foundation in order to be able to submit a Notification, by means of the form available after clicking on the "Submit Notification" button or an identical one on the Service;
 - b. be verified by the Foundation,
 - c. then activate the account on the Service by means of an activation link sent in an email to the email address provided by the Service Recipient.
2. The use of the electronic services necessary to submit the Form is free of charge.
3. The transmission of information within the Project is possible 24 (twenty-four) hours a day, 7 (seven) days a week, at the request of the Service Recipient.
4. The conclusion of the contract for the use of electronic services between the Service Recipient and the Foundation for the transmission of information within the Project occurs when:
 - a. activation of the account on the Service by clicking on the activation link - with regard to the service of registration and maintenance of the Account;
 - b. starting to fill in a Request after reading the dedicated information and clicking on the button "I want to fill in the Form" or the same.
5. In order to submit information to the Project, the Service Recipient must provide the mandatory data required. The provision of other data not marked as required is voluntary.
6. The submission of the Form is conditional on:
 - a. acceptance by the Service Recipient of the Regulations,
 - b. a declaration by the Service Recipient that the data provided is true,
 - c. if special categories of personal data are provided, consent to the processing of such data by the Foundation by indicating the relevant consent below the Form. Your consent is voluntary, but failure to do so will prevent you from submitting the Form,
 - d. read the information clause.
7. A Service Recipient may submit more than one Form under their account.
8. The Form uses an autosave mechanism and the Foundation allows the Service Recipient to save the form at any time using the "Save" button. The Foundation is entitled to direct an email to the email address of the Service Recipient 6 months after saving the Form, if it has not been sent to the Foundation, with a reminder to submit it. After this time, if the Service Recipient wishes to submit information as part of the Project, they will have to complete the Form from the beginning.
9. The contract for the use of Electronic Services is concluded for an indefinite period of time.
10. Agreements for the provision of Electronic Services are concluded in Polish or in another language provided by the Foundation, the choice of which is made by the Service Recipient.
11. The Service Recipient may terminate the agreement for the provision of Electronic Services at any time:
 - a. for account maintenance by sending such information to the Foundation at the e-mail address: contact@projectsunflowers.org
 - b. for using the Form by logging in to the Service and selecting the "Withdraw Form" option and then following the instructions provided.
12. The Foundation is entitled to terminate the Agreement at any time in the event that the Foundation ends its operations and services related to the Project, including the submission of Forms. In addition, the Foundation may terminate accounts that have not submitted a Form for a period of 6 months after the account has been activated, and such action does not require prior notice. In this case, the Service Recipient wishing to submit information under the Project in the future will have to fulfil again the conditions set out in § 4.1 of the Regulations.

§ 6. Service Recipient's obligations

1. The Service Recipient is obliged to use the Service and provide information on the Project in a manner consistent with the law and the Regulations, including:
 - a. use the Service in a manner that does not violate the rights of third parties, good practice or the law,
 - b. not include in the Form any misleading or unlawful content,
 - c. to use the services and the Service in a manner that does not interfere with their functioning,
 - d. not to transmit data, including personal data of third parties, without an appropriate legal basis, including the consent of such third parties.
2. The Foundation informs that the public nature of the Internet and the conclusion of contracts for the use of the services in order to transmit information within the framework of the Project, may involve the standard risks resulting from the use of the Internet, including the threat of obtaining, appropriating or modifying the Service Recipient's data by unauthorized persons. Consequently, the Service Recipient should use appropriate technical measures to minimise the risk, including anti-virus or identity protection software for Internet users.

§ 7. Liability of the Foundation

To the extent permitted by law, the Foundation shall not be liable for:

- a. acts and omissions of telecommunications operators and service providers used by the Service Recipient to access the Service and services,
- b. breaks or hindrances to the access to the Service and services caused by necessary technical interruptions, failures of telecommunication links or caused by vis maior,
- c. the Service Recipient's acts contrary to the Regulations, including damages caused to third parties as a result of the Service Recipient's use of the services contrary to the Regulations and the law,
- d. false data provided by the Service Recipient in the course of providing information within the framework of the Project, including towards third parties whose data was provided by the Service Recipient.

§ 8. Complaints

1. In matters related to the provision of services necessary for the transmission of information under the Project, the Service Recipient has the right to lodge a complaint. The complaint should contain at least the following information: name and surname of the Service Recipient, e-mail address of the Service Recipient, description of the circumstances justifying the complaint.
2. If the complaint does not contain the data indicated in para. 1 above, the Foundation is entitled to call on the Service Recipient to supplement the data. If the data is not completed, the complaint cannot be recognised by the Foundation.
3. Complaints can be addressed to the Foundation's address, i.e. Foundation Sunflowers with its registered office in Warsaw, Poland, at Siedmiogrodzka Street no. 5/51, 01-204 Warsaw, with the annotation "Complaint" or to the e-mail address: contact@projectsunflowers.org
4. Complaints will be considered by the Foundation within 14 days of receipt. The Foundation will inform about the manner of complaint consideration in a manner corresponding to the manner of complaint submission.

§ 9 Final provisions

1. The Foundation is the administrator of personal data provided in connection with the provision of information as part of the Project in accordance with the [Privacy Policy](#).
2. The Foundation is entitled to make changes to the Regulations for important reasons, in particular in the case of changes in the conditions of providing services necessary for the transmission of information as part of the Project, their suspension or termination in whole or in part, as well as in the case of changes in the law in the scope that affects the implementation of the provisions of the Regulations. Any changes to the Regulations are effective 14 days after the date on which the Service Recipient is informed of the planned change to the Regulations.
3. The law applicable to the obligations arising from the Regulations shall be Polish law and any disputes shall be settled by the competent Polish common courts.
4. In matters not covered by the Regulations, the provisions of Polish law shall apply, in particular the Act on Consumer Rights and the provisions of the Civil Code.
5. The Service Recipient who is a consumer has the possibility to use out-of-court ways of dealing with complaints and claims. Disputes concerning agreements concluded via the Internet may be resolved through mediation proceedings before the Provincial Inspectorates of Trade Inspection or through an arbitration court at the Provincial Inspectorate of Trade Inspection. The consumer can also use other methods of out-of-court dispute resolution and, for example, submit his/her complaint via the EU ODR online platform, available at: <http://ec.europa.eu/consumers/odr/>
6. The Regulations enter into force on 5 July 2023.