**Information Security Policy**

Document type - Policy

Applies -   to all programs and projects

Date of adoption - March 31, 2023

Date of next review and monitoring-  March 2024

**General provisions**

The accumulation of personal data of the CO "CF "SOS Civil Defense Headquarters" (hereinafter – the Organization) is carried out in accordance with the Law of Ukraine "On Personal Data Protection".

Personal data is stored under the following conditions:

**lawfulness**: personal data must be processed in a **lawful and transparent manner;**

**compatibility**: personal data must be collected for specific legitimate purposes and processed in accordance with them;

**adequacy and proportionality:** personal data must be adequate, not excessive, and relevant to the purposes of processing;

**accuracy**: personal data must be accurate and up-to-date;

**storage limitation**: personal data should not be stored for longer than provided by the consent of the personal data subject or the requirements of the laws of Ukraine;

 **the rights of access:** personal data must be processed in compliance with the rights of the personal data subject, in particular the right to access the data;

**security**: processed in a manner that ensures appropriate security of the personal data;

**cross-border protection:** personal data should not be transferred to foreign entities related to personal data without proper protection.

**Terminology**

**Anonymised data** means encrypting or removing personally identifiable data from data sets so that the person can no longer be identified.

**Consent** means any free and informed decision made without coercion, expressed and accepted for a specific purpose.

**Child** means any person under the age of 18.

**Data controller** means an employee of the Organization or a person representing a third party who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system.

**Data processing** – any action or set of actions which is related to the collection, registration, accumulation, storage, adaptation, modification, renewal, use and dissemination of information about an individual.

**Data protection –** the systematic application of a set of institutional, technical, physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data.

**Data subjects -** means a beneficiary of the Organization who can be directly or indirectly identified by the reference to a specific factor or factors. Such factors may include a name, an identification number, material circumstances and physical, mental, cultural, and economic or social characteristics to determine the beneficiary of the Organization.

**Electronic record** means any data storage system that records personal data.

**Beneficiary of the Organization** means any person receiving assistance or benefits from Organization's project.

**The Organization staff** means all persons working for the Organization on a temporary or permanent basis, as well as volunteers.

**Knowledge** means the ability to fully understand and appreciate the specified purpose for which personal data are collected and processed.

**Non-personal data** means any information that is not related to an identified or identifiable subject in respect of whom the information is collected.

**Paper record** means any printed or written document that contains personal data.

**Personal data** means any information relating to an identified or identifiable data subject that is recorded by electronic means or on paper.

 **Third party** means any natural or legal person, government or other entity that is not a party to the purpose for which personal data is collected and processed.

**Vulnerable groups** means any group or sector of society, including children, that are at exceptional risk of being subjected to discriminatory practices, violence, natural disasters, or economic hardships.

**Vulnerable person** means any beneficiary of the Organization that may lack the legal, social, physical or mental capacity to provide consent.

**Principles of Information Security which the Organization adheres**

1. **LAWFUL AND FAIR COLLECTION**

Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject about whom the information is collected.

1. **SPECIFIED AND LEGITIMATE PURPOSE**

The purpose(s) for which personal data are collected and processed should be specified and legitimate, and should be known to the data subject at the time of collection. Personal data should only be used for the specified purpose(s), unless the data subject consents to further use or if such use is compatible with the original specified purpose(s).

1. **DATA QUALITY**

Personal data sought and obtained should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.

1. **CONSENT**

Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter, and the condition and legal capacity of certain vulnerable groups and individuals should always be taken into account. If exceptional circumstances hinder the achievement of consent, the data controller should, at a minimum, ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose(s) for which personal data are collected and processed.

1. **TRANSFER TO THIRD PARTIES**

Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing.

1. **CONFIDENTIALITY**

Confidentiality of personal data must be respected and applied to all the stages of data collection and data processing, and should be guaranteed in writing. All Organization staff and individuals representing third parties who are authorized to access and process personal data, are bound to confidentiality.

1. **ACCESS AND TRANSPARENCY**

Data subjects should be given an opportunity to verify their personal data, and should be provided with access insofar as it does not frustrate the specified purpose(s) for which personal data are collected and processed. Data controllers should ensure a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.

1. **DATA SECURITY**

Personal data must be kept secure, both technically and organizationally, and should be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. The safeguard measures outlined in relevant Organization policies and guidelines shall apply to the collection and processing of personal data.

1. **RETENTION OF PERSONAL DATA**

Personal data should be kept for as long as is necessary, and should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled. It may however, be retained for an additional specified period, if required for the benefit of the data subject.

1. **APPLICATION OF THE PRINCIPLES**

These principles shall apply to both electronic and paper records of personal data, and may be supplemented by additional measures of protection, depending inter alia on the sensitivity of the personal data. These principles shall not apply to non-personal data.

1. **OWNERSHIP OF PERSONAL DATA**

The Organization shall assume ownership of personal data collected directly from data subjects or collected on behalf of the Organization, unless otherwise agreed, in writing, with a third party.

1. **OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES**

An independent body should be appointed to oversee implementation of these principles and to investigate any complaints, and designated data protection focal points should assist with monitoring and training. Measures will be taken to remedy unlawful data collection and data processing, as well as breach of the rights and interests of the data subject.

**Security levels and application of information security protocols**

**Level 1: Physical security** protects devices and data from physical threats, such as device theft, equipment damage, or data theft. To protect information at the physical security level, you should follow the following rules:

* Store devices and storage media in secure locations with limited access.
* Use passwords and other security methods to ensure secure access to devices and information.
* Disconnect and unplug devices that are not in use to prevent them from being damage and use for unauthorized purposes.

**Level 2: Network security** protects network connections and systems from unauthorized access, storage and transmission of information that could potentially be stolen, damaged or destroyed. The network security level includes special software tools that provide authentication, authorization and control of user access to network resources.

Network security includes protection against threats such as viruses, Trojans spyware and other malicious programs that can steal confidential information or cause damage to systems. To protect the network from such threats, we use antivirus programs.

**Level 3: Software security** - includes protection against various threats, such as viruses, worms, malware, data theft, etc. Ensuring security at this level includes regular software updates, installation of security programs, controlling access to data and other measures aimed at ensuring the security of information stored and processed in the system.

Director of CO "SOS Civil Defense Headquarters"