

CHARITABLE ORGANIZATION SPANBOND CHARITABLE FOUNDATION

Annex 1 to Order No. 7-org
dated 1 June 2026

APPROVED BY:
(signature / seal)
Oleksandra KARPENKO
CEO of the Foundation CO SPANBOND CF



PRIVACY AND PERSONAL DATA PROTECTION POLICY OF THE CHARITABLE ORGANIZATION SPANBOND CHARITABLE FOUNDATION

1. INTRODUCTION

This Privacy and Personal Data Protection Policy (hereinafter referred to as the "Policy") establishes the requirements and procedures for the collection, processing and protection of beneficiaries' personal data, as well as for the storage of information and the protection of information published on the public resources of the CHARITABLE ORGANIZATION SPANBOND CHARITABLE FOUNDATION (hereinafter referred to as the "Foundation" or "SPANBOND").

2. PURPOSE AND OBJECTIVES

The purposes of this Policy are:

- to ensure that SPANBOND's activities comply with the legislation of Ukraine and the requirements of the General Data Protection Regulation (GDPR) concerning the collection, processing and storage of the personal data of the Foundation's beneficiaries and employees;
- to establish mechanisms and procedures for ensuring the protection and confidentiality of the collection, processing and storage of personal data and information concerning the Foundation's beneficiaries and employees, and to raise the awareness and accountability of the members of the Foundation Team in the field of information security.

3. TERMS AND DEFINITIONS

Personal Data means any information relating to an identified natural person, including a Beneficiary or a Member of the Foundation Team.

The SPANBOND Team or the Foundation Team means persons engaged in the implementation of SPANBOND projects and programmes, including employees of the Foundation and service providers, whether individuals or individual entrepreneurs, engaged for a specified period under service agreements concluded in accordance with civil law.

Beneficiary means a person who directly receives goods or services under the Foundation's programmes. Persons covered by this term include vulnerable and affected population groups, particularly children, including refugees, internally displaced persons and other vulnerable persons, as well as members of the communities hosting them.

Processing of Personal Data means any operation or set of operations performed on personal data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction.

Personal Data Database means an organised collection containing beneficiaries' personal data and enabling such data to be systematised and accessed. The Personal Data Database also contains the personal data of SPANBOND employees required for the performance of their employment duties and for the Foundation's administrative and tax reporting obligations as an employer.

Owner of the Personal Data Database means SPANBOND, which owns and manages the personal data database containing the personal data of beneficiaries and members of the Foundation Team, as defined in this Policy.

CHARITABLE ORGANIZATION SPANBOND CHARITABLE FOUNDATION

Data Subject means a natural person to whom the personal data relate and who is identified or can be identified by means of such data.

Consent of the Data Subject means any documented, including written, freely given indication of the natural person's wishes by which they authorise the processing of their personal data for the stated purpose. The data subject's consent may also be incorporated into an employment agreement or a civil-law agreement.

Anonymisation of Personal Data means the removal of information that makes it possible to identify a person, as a result of which the data are transformed into data that may be used solely for statistical analysis.

Information Storage means maintaining information and the physical media on which it is stored in an appropriate condition.

Confidentiality of Information means a property of information whereby such information may not be accessed by an unauthorised user and/or process. Information remains confidential where the established rules governing access to it are observed.

4. RESPONSIBLE PERSONS AND SCOPE OF APPLICATION

This Policy applies to all SPANBOND employees, including full-time and part-time employees, employees holding primary positions and employees working concurrently.

The CEO of SPANBOND makes strategic decisions concerning the collection, processing, storage and transfer of personal data, confidentiality and information security.

The CEO of SPANBOND is responsible for ensuring the implementation of this Policy with regard to the secure and proper collection, storage, processing and transfer of personal data, confidentiality and information security, as well as for responding to requests, including the development and implementation of information security policies and procedures.

The CEO of SPANBOND is responsible for the proper storage of and restricted access to physical documents containing personal data, as well as for their transfer and processing, and submits proposals regarding updates to this Policy.

The CEO of SPANBOND is responsible for familiarising SPANBOND employees with this Policy and for taking measures to raise the awareness of the SPANBOND Team regarding data protection and security in the processing and storage of personal data, confidentiality and information security.

The CEO of SPANBOND, Project Managers and heads of the Foundation's structural units and areas of activity shall take effective measures concerning the collection, processing and storage of personal data and confidentiality and may not transfer personal data to other parties at their request without the written authorisation of the CEO of SPANBOND.

The installation of software and antivirus applications and the updating of operating systems on all SPANBOND network-connected devices shall be carried out only with the approval of the CEO of SPANBOND.

The CEO of SPANBOND shall provide oversight and operational supervision over the Foundation's processing of personal data, confidentiality and information security.

5. CONFIDENTIALITY, STORAGE AND PROTECTION OF INFORMATION

A corporate email account shall be created for every SPANBOND employee. Such an account is the property of SPANBOND and shall be protected by a password, which the employee may not disclose to any other person. All information contained in the account is confidential and may not be disclosed to third parties. Employees may use their corporate email accounts solely for work-related purposes. Private email correspondence through corporate accounts is not permitted.

Together with a corporate email account, an employee may be granted access to the Foundation's cloud-based information storage systems. Access to such systems shall also be protected by a password, and the copying or dissemination of the information stored therein is prohibited. Each user of a cloud-based storage system shall be granted access only to the extent necessary for the performance of their employment duties and no more, in accordance with the Principle of Least Privilege.

From the moment they receive a corporate email account of the Foundation, SPANBOND employees shall comply with the confidentiality requirements applicable to information distributed through this channel. They shall not disclose confidential information to third parties without the appropriate authorisation.

Upon termination of the employment relationship between an employee and SPANBOND, the employee's account shall be deactivated on the date of termination. The account shall be archived two weeks later. The CEO of SPANBOND shall have access to the deactivated and archived corporate email account.

CHARITABLE ORGANIZATION

SPANBOND CHARITABLE FOUNDATION

Where SPANBOND provides an employee with a laptop, computer or tablet for the performance of their employment duties, access to the device shall be restricted and protected by a password.

To preserve information and maintain confidentiality, the CEO of SPANBOND shall arrange regular backups of employees' corporate email accounts and cloud-based storage systems. Regular backups shall be performed to prevent data loss. Backup copies shall be stored in a secure location separate from the primary data storage location.

When publishing any information on public resources, the confidentiality of personal data and SPANBOND's confidential information shall be protected. This applies to the Foundation's social media pages and corporate website.

Access to public resources on which SPANBOND information is published shall be restricted and granted only to authorised persons.

The scope of confidential information and the extent of access to personal data granted to each SPANBOND employee shall be determined by the employee's job description, which shall be communicated to the employee on their first working day.

Any information that becomes known to a Foundation Team Member in connection with the performance of obligations under an agreement with the Foundation or the performance of their employment duties, and the disclosure of which may cause harm to any third party, constitutes a trade secret and may not be disclosed or published without the prior consent of the relevant data subject or owner of the information. The party responsible for disclosing such information shall be held liable in accordance with the applicable legislation of Ukraine.

Confidential information includes information that has actual or potential value to SPANBOND, is unknown to third parties and is protected by the Foundation through appropriate confidentiality measures, as well as other information that does not constitute a trade secret but has been designated by SPANBOND as confidential.

Foundation Team Members shall not disclose or reveal to third parties any confidential information provided to them by the Foundation during the term of their employment agreement or employment relationship with the Foundation and for two years following its termination. They shall not use such information for any purpose other than that for which it was provided by the Foundation without the Foundation's prior written consent.

Personal data obtained by Foundation employees in the performance of their employment duties shall remain confidential indefinitely. Where necessary, the Foundation reserves the right to monitor the use and storage of confidential information by Foundation Team Members.

Foundation Team Members shall maintain the confidentiality of negotiations, correspondence and other activities relating to contractual terms and shall not disclose such information to third parties without the written consent of the other party.

6. PERSONAL DATA DATABASES

SPANBOND processes personal data for the implementation of the Foundation's programmes and projects, the protection of beneficiaries and Foundation Team Members, and other purposes established by the legislation of Ukraine and the requirements of the General Data Protection Regulation (GDPR).

The legal grounds for exercising the right to use personal data are:

1. the data subject's consent to the processing of their personal data, provided in writing or by electronic means;
2. authorisation to process personal data granted to SPANBOND under the legislation of Ukraine and the requirements of the General Data Protection Regulation (GDPR), solely for the exercise of its powers.

The Foundation owns and processes the following personal data databases:

1. Beneficiaries' Personal Data Database, which contains basic information concerning SPANBOND beneficiaries, including their first and last names, contact details, information concerning the support received, and other relevant information.

The purpose of processing the Beneficiaries' Personal Data Database is to comply with applicable legislation, exercise the rights granted to SPANBOND by law, and ensure the proper administration of tax matters and matters relating to accounting, auditing and other related activities.

CHARITABLE ORGANIZATION

SPANBOND CHARITABLE FOUNDATION

2. Foundation Team Members' Personal Data Database.

The Foundation Team Members' Personal Data Database contains information concerning their last name, first name and patronymic, date and place of birth, home and mobile telephone numbers, email address, registered address, passport details, taxpayer registration number, education, marital status, children, citizenship, possession of an international passport, possession and category of a driving licence, employment history and any other data required for the exercise of employment rights and benefits and for the conclusion of service agreements.

The purpose of processing the Foundation Team Members' Personal Data Database is to maintain personnel records and prepare statutory, internal, statistical, administrative and other information in accordance with applicable legislation and the Foundation's internal standards and policies; to manage personnel and relationships with contracting parties, including service providers who are natural persons or individual entrepreneurs; and to prepare SPANBOND's internal documents concerning the exercise of rights and performance of obligations established by law in the areas of employment relations, social protection and civil-law relations.

As the owner of the personal data databases of beneficiaries and SPANBOND Team Members, the Foundation undertakes to use such data solely for the specified purposes established by its Charter or other legal documents and in accordance with the principles of lawfulness, fairness and transparency.

The Foundation shall not transfer the personal data of beneficiaries or Foundation Team Members to third parties without appropriate legal grounds, such as the beneficiary's consent or a requirement established by law.

The Foundation may transfer personal data to third parties solely upon the instruction of the CEO of SPANBOND.

The transfer of personal data shall be based on an agreement or contract, or on other mechanisms documented in writing that guarantee an adequate level of protection for such data and ensure compliance with the personal data protection legislation of Ukraine and the requirements of the General Data Protection Regulation (GDPR).

7. RESTRICTED ACCESS TO PERSONAL DATA AND THE RIGHTS OF DATA SUBJECTS

The Foundation shall ensure that access to the personal data of beneficiaries and Foundation Team Members is restricted to employees who require authorised access to such data within the scope established by their job descriptions.

Access to personal data shall be granted only to the extent necessary for the performance of specified tasks and duties relating to the implementation of the Foundation's projects and programmes, the performance of concluded agreements and the employment duties of SPANBOND employees.

SPANBOND, acting through its CEO, shall provide regular training and instruction to employees concerning the use and processing of personal data in accordance with applicable legislation and the Foundation's policies at least once a year.

SPANBOND employees who have access to the personal data of beneficiaries and Foundation Team Members shall maintain confidentiality and take all necessary security measures to protect such data in accordance with this Policy, the legislation of Ukraine and the General Data Protection Regulation (GDPR).

Data subjects have the right to the protection and use of their personal data in accordance with the legislation of Ukraine and this Policy.

Data subjects have the following rights:

- Right to information: Data subjects have the right to be informed that their personal data are being collected and processed, the purposes of processing, the categories of data recipients and the legal basis for processing.
- Right of access: Data subjects have the right to access their personal data stored in the Foundation's personal data databases and to obtain copies of such data by submitting a written request.
- Right to rectification: Data subjects have the right to request the rectification of inaccurate or incorrect personal data relating to them.
- Right to erasure: Data subjects have the right to request the erasure of their personal data from the Foundation's personal data databases where such data are no longer required for the stated purposes or where their processing is unlawful.
- Right to restriction of processing: Data subjects have the right to restrict the processing of their personal data in certain circumstances, including where the processing is unlawful or the data subject objects to the processing.

CHARITABLE ORGANIZATION

SPANBOND CHARITABLE FOUNDATION

- Right to data portability: Data subjects have the right to receive the personal data they have provided to SPANBOND in a structured, commonly used format and to transmit those data to another personal data controller without hindrance from the Foundation, where the processing is based on consent or a concluded agreement and is carried out by automated means.
- Right to withdraw consent: Where personal data are processed on the basis of the data subject's consent, the data subject has the right to withdraw their consent at any time. Withdrawal of consent shall not affect the lawfulness of processing carried out before the consent was withdrawn. The data subject shall understand that withdrawal of consent may result in the termination of employment relations, contractual civil-law relations or the discontinuation of assistance provided to them as a beneficiary.
- Right to lodge a complaint: Data subjects have the right to lodge complaints with the competent supervisory authorities where they believe that their personal data protection rights have been violated.
- Other rights: Data subjects also have any other rights established by personal data protection legislation.

Data subjects may exercise their rights by contacting SPANBOND in accordance with Article 16 of the Law of Ukraine "On Personal Data Protection". The Foundation shall ensure that such rights can be exercised and shall respond appropriately to data subjects' requests within the time limits and in accordance with the requirements established by law.

8. PROCEDURE FOR PROCESSING PERSONAL DATA

Personal data shall be processed in accordance with applicable legislation, the principles of personal data confidentiality and security, and the requirements of the General Data Protection Regulation (GDPR). Personal data shall be collected and processed on the basis of consent provided in the prescribed form set out in Annex 1 or on the basis of consent incorporated into the relevant employment agreement or civil-law agreement.

Personal data may be processed using automated systems used by SPANBOND, including CRM systems, as well as without the use of automated systems.

SPANBOND may generate personal data independently in the form of individual personnel orders and directives. Such documents constitute confidential information and may be disclosed only in the cases provided for by the applicable legislation of Ukraine.

SPANBOND shall implement appropriate measures to protect personal data against unauthorised access, accidental loss or damage, destruction, alteration, disclosure or unlawful processing. Such measures shall include continuously updating the security of automated personal data storage systems and providing a safe and secure location in the Foundation's office premises or archives for the storage of personal data in non-automated form.

Personal data may be processed by SPANBOND or, on its instructions, by third parties pursuant to concluded agreements or contracts or on other lawful grounds established by applicable legislation.

SPANBOND shall store personal data in automated and non-automated form for the period required to achieve the purposes of processing under the relevant employment agreement or civil-law agreement or for the implementation of the relevant project, unless otherwise provided by law or by an agreement with the data subject.

The processing of personal data may be terminated at the initiative of the data subject, upon a written request from the competent supervisory authorities or where required by applicable legislation.

Personal data may be transferred to third parties only in the cases provided for by law or by a project implementation agreement and in compliance with personal data confidentiality and security requirements.

In the event of a personal data security breach that may result in unauthorised access to, loss, alteration or damage of such data, the Foundation shall notify the competent supervisory authority and the relevant data subjects in accordance with applicable legislation.

The Foundation shall provide appropriate conditions for data subjects to exercise their rights, including the rights to access personal data, rectify inaccurate or incorrect data and request the erasure of data.

Consent to the processing of personal data may be incorporated into other Foundation documents signed by the beneficiary, provided that the beneficiary is informed of the collection of their personal data.