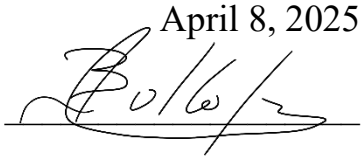
TECHNOLOGY OF PROGRESS

APPROVED
Executive Director
NGO «Technology of Progress»
Zadvornyy V.V.
April 8, 2025



Approved
By Order No. 2-D dated April 8, 2025

Approved
By the Decision of the Extraordinary General Meeting No. 1-P dated April 8, 2025

PRIVACY POLICY

Kyiv, 2025

1. Purpose of the Document

1.1 This document of the Non-Governmental Organization «Technology of Progress» (hereinafter – the «Organization») defines the key principles and requirements aimed at protecting confidential information held by the Organization, including the protection of personal data and any other confidential information of individuals cooperating with the Organization.

2. Definitions

2.1 Personal Data – information or a set of information about an individual who is identified or can be specifically identified.
2.2 Confidential Information – information that is held, used, or controlled by certain individuals or legal entities and is disclosed at their discretion under the conditions they set.
2.3 Confidentiality of Information – the property of information to be protected from unauthorized access.
2.4 Information Confidentiality Regime – legal, organizational, technical, and other measures to protect personal data.
2.5 Owner of Confidential Information – a person who lawfully possesses confidential information, restricts access to it, and establishes a confidentiality regime in relation to this information.
2.6 Counterparty – a party to a civil law contract to whom the owner of confidential information has disclosed such information under the condition of maintaining its confidentiality.

3. Confidential Information

3.1 The following data (information) are considered confidential:
3.1.1 Information contained in the financial, legal, and other documents of the Organization that constitute its internal record-keeping.
3.1.2 Terms of the Organization's contracts with its Counterparties, any other details of relations with Counterparties, and any other information about Counterparties, subject to prior agreement on confidentiality.

4. Establishment of the Confidentiality Regime

4.1 The confidentiality regime of information is considered to be established after the completion of the relevant legal procedures for applying the confidentiality regime to such information.

5. Rights and Obligations of the Organization

5.1 The Organization has the right to:
5.1.1 establish, modify, and cancel the confidentiality regime in writing in accordance with applicable law;
5.1.2 use information constituting a trade secret and/or confidential information for its own purposes in a manner that does not contradict the law;

5.1.3 permit or deny access to confidential information and determine the rules and conditions for such access;
5.1.4 introduce confidential information into civil circulation based on agreements that include confidentiality protection terms;
5.1.5 require legal entities and individuals who have received access to confidential information, as well as government authorities, other state bodies, and local self-government bodies to which confidential information was provided, to comply with confidentiality obligations;
5.1.6 require persons who have accessed confidential information accidentally or mistakenly to maintain its confidentiality;
5.1.7 amend the Privacy Policy to further improve the security system in accordance with applicable law.

5.2 The Organization is obliged to:

5.2.1 protect its rights under applicable legislation of Ukraine, this Policy, employment, and civil contracts in case of disclosure, illegal receipt, or unauthorized use by third parties of confidential information, including the right to claim compensation for damages caused by the violation of these rights.

6. Protection of Confidentiality of Information

6.1 To ensure the protection of confidentiality of information, employees, members of the Organization, and other officials who, according to the specifics of their cooperation with the Organization, have access to confidential information, are required to:
6.1.1 assume a written obligation not to disclose confidential information;
6.1.2 not disclose information that constitutes confidential information;
6.1.3 continue to not disclose the aforementioned confidential information even after the termination of contractual (employment) obligations with the Organization;
6.1.4 compensate for any damage caused by the disclosure of information constituting confidential information.

7. Procedure for Storage, Use, Provision, and Accounting of Confidential Information

7.1 Paper and electronic sources containing the Organization’s confidential information shall be stored during non-working hours only in safes or lockable boxes; electronic databases storing information shall be encrypted with appropriate security passwords.
7.2 When working with electronic sources, without prior consent from the Organization’s management, it is prohibited to:
7.2.1 make copies of electronic sources containing confidential information, or transfer them to persons who do not have access to confidential information;
7.2.2 disclose confidential information to employees of the Organization or other persons who do not have access to such confidential information.
7.3 Information constituting confidential information of the Organization may be provided to contractors upon concluding agreements, upon their request, and with prior consent from the owners of personal data.

7.4 Information containing confidential information may be provided exclusively by the Executive Director of the Organization or persons authorized to act on their behalf, only upon a written request from representatives of state executive authorities, supervisory, and law enforcement agencies.

8. Final Provisions

8.1 This Policy comes into effect from the date of its approval by the Executive Director of the Organization.