

APPROVED
By Order of the General Director
of KIBERTEKH LLC
Dated December 25, 2024, No. 25/12/24-1

Personal Data Policy

1. Introduction

This Personal Data Policy (hereinafter referred to as the “Policy”) has been developed in accordance with Clause 2 of Article 18.1 of Federal Law No. 152-FZ of July 27, 2006 “On Personal Data” and applies to all personal data processed by KIBERTECH LLC (hereinafter the “Company”), including data collected from employees (in the course of employment), as well as clients and contractors (in the course of business activities).

This Policy aims to ensure the protection of human and civil rights and freedoms in the processing of personal data, including the right to privacy, personal and family confidentiality.

The Policy outlines the principles of personal data processing and protection, the legal basis for such processing, the rights of data subjects, and other relevant provisions.

This Policy is made publicly available via Company notice boards and the official website.

To implement this Policy and comply with applicable data protection laws, the Company has adopted internal regulations and administrative documents.

2. Definitions

Personal data – any information relating directly or indirectly to an identified or identifiable natural person (data subject).

Personal data made publicly available by the data subject – personal data to which access is granted to an unlimited number of persons, based on the data subject’s consent, in accordance with the law.

Data Controller (Operator) – KIBERTECH LLC, Tax ID 1655475060, Government Registration No. 1221600026185, which independently or jointly with others organizes and/or processes personal data, and determines the purposes, scope, and means of such processing.

Processing of personal data – any operation or set of operations performed with or without automation, including collection, recording, systematization, accumulation, storage, updating, retrieval, usage, transfer, anonymization, blocking, deletion, and destruction.

Disclosure – actions aimed at providing access to personal data to a specific person or group.

Blocking – temporary suspension of personal data processing (except where processing is necessary for data clarification).

Destruction – actions making it impossible to restore personal data in the information system and/or resulting in the destruction of physical data carriers.

Anonymization – actions making it impossible to identify a data subject without additional information.

Information system – a set of databases, software, and technical means used to process personal data.

Cross-border data transfer – transfer of personal data to a foreign state or entity.

3. Principles of Personal Data Processing

The Company processes personal data using both automated and manual methods based on the following principles:

Lawfulness and fairness – processing is conducted in compliance with legal requirements and fairness;

Purpose limitation – processing is limited to specific, legitimate purposes;

Data compatibility – combining personal data from incompatible databases is prohibited;

Data relevance – only data necessary for the stated purposes is processed;

Accuracy – data is kept accurate, up-to-date, and relevant to processing purposes;

Storage limitation – data is stored only as long as necessary for its purpose or as required by law;

Data deletion – data is deleted or anonymized once the processing purpose has been achieved or is no longer relevant.

4. Legal Basis for Processing

The Company processes personal data for the following purposes:

- Execution of its statutory functions and legal obligations;
- Fulfillment and conclusion of employment or civil law contracts;
- HR management, tax, and pension accounting;
- Communication with clients and contractors;
- Improvement of services and direct marketing (subject to consent);
- Statistical and analytical purposes (with anonymized data).

5. Purposes of Data Processing

Personal data is processed by the Company based on:

- The Constitution of the Russian Federation and international treaties;
- Federal Law No. 152-FZ “On Personal Data” and other federal laws including (but not limited to) the Civil Code, Labor Code, Tax Code;
- Other applicable laws governing employment, pensions, insurance, military service, accounting, etc.;
- Company bylaws and contracts with data subjects;
- Consent provided by data subjects.

6. Conditions and Methods of Processing

- Personal data is processed in accordance with Russian law, both automatically and manually.
- Only authorized personnel with job-related responsibilities are allowed to process personal data.
- Disclosure to third parties is prohibited without the subject's consent, unless required by law.
- Transfers to government authorities and other legal entities are done strictly in accordance with legal requirements.
- Data of Russian citizens collected online is stored and processed using databases located within the Russian Federation.

7. Third-Party Processing and Responsibility

If the Company outsources data processing to another party:

- The Company remains fully liable for the processor's actions;
- The processor must comply with all legal obligations, ensure confidentiality, and protect the data;
- A formal agreement will outline the scope, purpose, and data protection requirements in accordance with Article 19 of Federal Law No. 152-FZ.

8. Data Retention and Storage

Personal data is processed from the time it is received by the Company until:

- Unlawful processing is discovered and cannot be corrected within 3 business days;
- The purpose of processing has been achieved or is no longer valid;
- Consent is withdrawn (unless processing is otherwise legally required);
- The Company ceases operations.

For marketing purposes, data may be retained indefinitely until consent is withdrawn.

9. Data Destruction

Personal data must be destroyed when:

- Unlawful processing cannot be rectified within 10 business days;
- The purpose of processing has been fulfilled or is no longer applicable (within 30 days);
- Consent is withdrawn and no legal basis for further processing exists (within 30 days).

If immediate destruction is not possible, the data must be blocked and destroyed within 6 months.

10. Rights and Obligations

The Company may:

- Protect its interests in court;
- Disclose data to authorities when legally required;
- Deny access to personal data in cases defined by law.

The Company is obligated to:

- Grant data subjects access to their data;
- Correct or delete inaccurate, outdated, or unlawfully obtained data;
- Comply with Russian data protection laws.

Data Subjects have the right to:

- Request access, correction, blocking, or deletion of their personal data;
- Request information on data sources and storage periods;
- Be notified of corrections or deletions made;
- File complaints with supervisory authorities or courts.

Data Subjects are obligated to:

- Provide accurate and complete personal data;
- Notify the Company of any changes;
- Comply with applicable legal requirements.

11. Data Protection Measures

The Company protects:

- Paper and electronic records containing personal data;
- Personal data stored in databases and IT systems;
- All data from unauthorized access, destruction, modification, copying, or disclosure.

Protection is based on principles of:

- **Legality** – compliance with regulatory requirements;
- **Complexity** – combination of technical and organizational safeguards;
- **Continuity** – protection at all stages and under all operating conditions;
- **Timeliness** – measures are taken before processing begins;
- **Control** – continuous monitoring of data protection systems.

12. Final Provisions

This Policy is publicly available and may be updated based on changes in legislation. Revisions are made at least once every three years or as required by law.

Compliance with this Policy is monitored by the person responsible for data processing within the Company.