

PERSONAL DATA PROCESSING AND PROTECTION POLICY IPHARMA LLC

1. General provisions

1.1. This Personal Data Processing and Protection Policy (hereinafter - "the Policy") is compiled in accordance with Paragraph 2 Article 18.1 of the Federal Law No. 152-FZ "On Personal Data" dated July 27, 2006, as well as with other laws and regulations of the Russian Federation related to personal data processing and protection and applies to all personal data (hereinafter – "the Data") that an Organization (hereinafter – "the Operator") can receive from a personal data subject who is a party to a civil contract, from an Internet user (hereinafter – "the User") while using any IPHARMA LLC websites, facilities, support, programs, products or services, as well as the personal data subject, which is in the employ of the Operator (hereinafter – "the Employee").

1.2. The Operator ensures the protection of the personal data processed from unauthorized access and disclosure, misuse or loss in accordance with the requirements of the Federal law No. 152-FZ "On Personal Data" dated July 27, 2006.

1.3. The Operator has the right to modify this Policy. When introducing changes, the date of the last revision update is indicated in the Policy header. The new version of the Policy comes into force from the moment it is posted on the website, unless otherwise provided by the new version of the Policy.

2. Terms and abbreviations

Personal data – any information that is related directly or indirectly to an identified or an identifiable individual (personal data subject).

Personal data processing – any actions (operations) or sets of actions (operations) including collection, recording, systematization, accumulation, storage, validation (updating, modification), extraction, use, transfer (distribution, provision, access), blocking, deletion, and destruction of personal data with and without the use of personal data automated processing systems.

Automated personal data processing – personal data processing using computer aids.

Personal data information system (PDIS) – the total of personal data contained in databases, as well as information technologies and facilities, which ensure its processing.

Personal data made publicly available by the personal data subject – the personal data accessed to an unlimited number of persons by the personal data subject or at his request.

Personal data blocking – temporary interruption of personal data processing (except where processing is required for personal data update).

Personal data destruction – actions making it impossible to restore personal data volume in the personal data information system and/or resulting in the elimination of tangible media.

Operator – the organization that independently or jointly with other parties organizes and (or) conducts personal data processing, as well as defines purposes of processing the personal data, which is subject to processing, and actions (operations) conducted with personal data. The Operator is IPHARMA LLC, located at: 121205, Russia, Moscow, Skolkovo Innovation Center, 40 Bolshoy Boulevard, floor 3, office XXXIII, room 77.

3. Personal data processing

3.1. The collection of personal data.

3.1.1. All personal data should be obtained from the subject. If the subject's personal data can only be obtained from a third party, then the subject must be notified or the consent must be obtained.

3.1.2. The Operator shall inform the subject about the purposes, expected sources and methods of personal data collection, the nature of the personal data to be collected, the list of actions with personal data, the consent duration and the procedure for its withdrawal, as well as the consequences of the subject's denial of written consent.

3.1.3. The documents containing personal data are created by:

- copying of original documents (passport, diploma, TIN certificate, pension certificate, etc.);
- an entry to accounting forms;
- obtaining the originals of necessary documents (employment record book, medical report, characteristics, etc.).

3.2. Personal data processing.

3.2.1. Personal data processing is carried out:

- with the consent of the personal data subject to the processing of his personal data;
- when the personal data processing is necessary for the exercise and performance of the functions, powers and duties assigned by the legislation of the Russian Federation;
- when processing the personal data accessed to an unlimited number of persons by the personal data subject or at his request (personal data made publicly available by the personal data subject).

3.2.2. Purposes for personal data processing:

- realization of civil law relations;
- contact with the User in connection with filling out the feedback form on the site, including sending notifications, requests and information relating to the site usage;
- depersonalization of personal data to obtain depersonalized statistical data that are transferred to a third party for conducting the study, execution of activities and performing services on behalf of the Operator.

3.2.3. Categories of personal data subjects.

Personal data are collected for the following categories of personal data subjects:

- employees;
- former employees;
- job applicants;
- individuals who are civil law contractors;
- Website users.

3.2.4. Personal data processed by the Operator:

- the data obtained in the exercise of the labor relations;
- the data obtained for the job applicants' selection;
- the data obtained in the exercise of the civil law relations;
- the data obtained from the Website users.

3.2.5. The processing of personal data can be:

- automated;

- non-automated.

3.3. Personal data storage.

3.3.1. The personal data of subjects can be collected, further processed and stored both on paper and in electronic form.

3.3.2. The personal data recorded on paper is stored in locked cabinets or locked rooms with restricted access.

3.3.3. The personal data of subjects processed using automation tools for different purposes are stored in different folders.

3.3.4. It is not allowed to store and place documents containing personal data in open electronic directories (file sharing sites) in PDIS.

3.3.5. The personal data shall be stored in the form allowing to identify a personal data subject only as long as is needed for personal data processing, and it is subject to destruction after the purposes of processing are achieved, or when there is no further need to achieve such purposes.

3.4. Personal data destruction.

3.4.1. The destruction of documents (electronic media) bearing the personal data are carried out using the following methods: burning, mutilation (chopping), chemical decomposition, pulping or pulverizing. Shredding is also allowed for destruction of paper documents.

3.4.2. The personal data on electronic media is destroyed by erasing or formatting of the storage medium.

3.4.3. The destruction of personal data are documented by a certificate of electronic media destruction.

3.5. Personal data transmission.

3.5.1. The Operator transfers personal data to third parties in the following cases:

- a subjected gave his/her consent;
- the transfer is envisaged in Russian or any other applicable laws and regulations under the legally established procedures.

3.5.2. Listed individuals and entities to which personal data are transferred.

- Pension fund of the Russian Federation (on legal grounds);
- Tax authorities of the Russian Federation (on legal grounds);
- Social Insurance Fund of the Russian Federation (on legal grounds);
- Territorial Fund of Compulsory Medical Insurance (on legal grounds);
- Health Maintenance Organization for compulsory and voluntary medical insurance (on legal grounds);
- Banks for payroll (under the contract);
- Agencies of the Ministry of Internal Affairs of the Russian Federation in cases established by law.

4. Personal data protection

4.1. The Operator created a personal data protection system (PDPS), consisting of subsystems of legal, organizational and technical protection, in accordance with regulatory requirements.

4.2. The subsystem of legal protection is a complex of legal, organizational, administrative and regulatory documents that ensure the creation, operating and improvement of the PDPS.

4.3. The subsystem of organizational protection includes the management of the PDPS organizational structure, the licensing system, and the data protection when working with employees, partners and third parties.

4.4. The subsystem of technical protection includes a complex of technical, software, hardware and software tools ensuring the protection of personal data.

4.4. Basic personal data protection measures used by the Operator are:

4.5.1. Appointment of a person responsible for the personal data processing, who organizes the processing of personal data, along with training, instructing, and internal control over the company's and employees' compliance with the requirements to the personal data protection.

4.5.2. Determining the current threats to the personal data protection during their processing in the PDIS, and developing the measures and activities for the personal data protection.

4.5.3. Development of a personal data protection policy.

4.5.4. Establishing the rules for access to personal data processed in the PDIS, as well as ensuring registration and accounting of all actions performed with personal data in the PDIS.

4.5.5. Establishing individual passwords for the employees to access the data system in accordance with their responsibilities.

4.5.6. Application of the procedures for conformity assessment of the data protection tools that were carried out properly.

4.5.7. Certified anti-virus software with regularly updated databases.

4.5.8. Compliance with the terms ensuring the safety of personal data and excluding an unauthorized access.

4.5.9. Detecting unauthorized access to personal data and taking actions.

4.5.10. Recovery of personal data modified or deleted due to unauthorized access.

4.5.11. Training the Operator's employees, directly administering the personal data processing, on the legislative provisions of the Russian Federation regarding the personal data, including the requirements for the personal data protection, documents defining the Operator's policy regarding the personal data processing, and local regulations on the personal data processing.

4.5.12. Implementation of internal control and audit.

5. Rights and obligations

5.1. Rights of the personal data subject.

A subject has the right to access his/her personal data and the following information:

- confirmation of the fact of personal data processing by the Operator;
- legal grounds and purposes of personal data processing;
- purposes and personal data processing procedures used by the Operator;
- name and location of the Operator, information on the persons (except for the Operator employees) who have access to personal data or to whom personal data may be disclosed according to an agreement with the Operator or to the Federal Law;
- personal data processing limits, including a storage duration;
- procedure for exercising of the personal data subject's rights provided for by the Federal Law;
- name of the company or full name and address of a person processing personal data on behalf of the Operator, if the processing is assigned or is planned to be assigned to a third party;
- communications with the Operator and addressing requests;

- appealing against Operator's actions or lack of actions.

5.2. Obligations of the Operator.

The Operator shall:

- provide information on the personal data processing when collecting personal data;
- notify the personal data subject if the personal data was received not from the personal data subject;
- explain the consequences in case of refusing to provide personal data to the subject;
- publish or otherwise provide unrestricted access to the document defining its policy regarding the personal data processing, and to information about the requirements implemented to the personal data protection;
- assume required legal, organizational and technical measures to protect personal data from unauthorized or accidental access, destruction, modification, blocking, copying, disclosure, distribution, and from any other inappropriate actions in relation to personal data;
- reply on queries and requests of personal data subjects, their representatives and an authorized body for the protection of the personal data subjects' rights.