ITMO University Personal Data Processing Policy ITMO University

General provisions

1.1 ITMO University Personal Data Processing Policy ITMO University (hereinafter Policy) determines the policy of the federal state autonomous higher education establishment “Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (state registration number 1027806868154, tax identification number 7813045547, address: Saint Petersburg, Kronversky pr. 49, hereinafter Operator) as regards to processing of personal data and defines among others, as list of actions conducted by the Operator to protect personal data.

1.2 The policy is approved and published on the website https://icps2018.net (hereinafter -"Site") in compliance with the Operator with Part 2 of Article 18.1 of the Federal Law of July 27, 2006 N 152-FZ "On Personal Data" (hereinafter referred to as "Federal Law") that requires to publish in the information-telecommunication network a document that defines the Operator's policy on processing of personal data, and information on the requirements for the protection of personal data, as well as to ensure access to the specified document using an appropriate information and telecommunication network.

1.3 The policy was developed considering the requirements of the Russian Federation in the field of personal data. The terms used in the Policy should be understood as defined in the Federal Law, if unless stipulated differently in the Policy.

1.4 The Policy is available to any user of the Internet by accessing the link https://icps2018.net/netcat_files/userfiles/official/policy.pdf

1.5 The Operator processes users’ personal data based on the following principles:

- Processing of personal data is carried out by the Operator on a legal and fair basis;
- Processing of personal data is limited to achieving specific, pre-defined and legitimate purposes. The Operator does not process personal data incompatible with the purposes of personal data collection;
- Combining databases containing personal data processed for incompatible purposes is not allowed;
- Operator can only process personal data that meet the objectives of their processing,
- The scope of volume of personal data processed by the Operator correspond with the declared objectives of the process;
- Processed personal data is not excessive to the declared purposes of the processing;
- Accuracy, sufficiency and in some cases, relevance to the purposes of the processing must be ensured when processing personal data;
- Operator must take the necessary measures to delete and update incomplete or inaccurate data;

- The storage of personal data is carried out in a form that allows to identify the subject of the personal data, no longer than needed for the purposes of processing, if the period of personal data storage is not established by federal law, or a contract, a party in which is a beneficiary or a guarantor under which is the subject of the personal data. The processed personal data must be destroyed or depersonalized after the objectives for processing are met or if these objectives are no longer relevant, unless otherwise stipulated by federal law.

2. Rights of the subject of personal data to access his personal data

2.1 The subject of personal data has the right to receive the following information:

- Confirmation of the fact of personal data processing by the Operator;
- Legal grounds and objectives for the processing of personal data;
- Objectives and methods of processing personal data;
- Name and location of the Operator, information about the persons (for the Operator's employees) who have access to personal data or personal data on the basis of a contract with the Operator or on the basis of federal law;
- Processed personal data relating to corresponding to the subject of personal data, the source of their receipt if there is no other procedure for submitting such data stipulated by federal law;
- Length of the period for processing of personal data, including the length of their storage;
- The order by which the personal data subject can exercise his or her rights as stipulated by the federal law;
- Information about actual or expected transboundary data transmission;
- Name or surname, name, patronymic and address of the person, carrying out the processing of personal data on behalf of Operator, if the processing is entrusted or will be entrusted to such a person;
- Other information provided for by the legislation of the Russian Federation.

2.2. The right of the subject of personal data to access his personal data may be limited in cases provided for by law of the Russian Federation.

3. Requirements for personal data protection implemented by the Operator

3.1. During the processing of personal data, the Operator takes all necessary legal, organizational and technical measures to protect personal data from unauthorized or accidental access, destruction, modification, blocking, copying, providing, distributing, as well as from other illegal actions in relation to personal data.

3.2 Ensuring the security of personal data is achieved, in particular, by:

1) Definition of threats to the security of personal data while being processed by personal data information systems;

2) Use of organizational and technical measures to ensure safety of personal data while being processed by personal data information systems necessary to meet the requirements for protection of personal data as established by the Government of the Russian Federation;

3) Use of information protection means evaluated by the specified procedure;

4) Evaluation of the effectiveness of personal data security measures prior to commissioning a personal data information system;

5) Accounting for computer storage of personal data;

6) Detection of unauthorized access to personal data and taking action;

7) Recovery of personal data modified or destroyed due to unauthorized access;

8) Establishing rules for access to personal data processed by the personal data information system, as well as ensuring registration and accounting of all actions performed with personal data in the personal data information system;

9) Control over the measures taken to ensure safety of personal data and the level of security of personal data information systems.