Annex 2 to the Data Processing Agreement (DPA)

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the Data Processor to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

1. Technical and Organization Measures

General principles

1.1. According to the nature of personal data stored by the Data Processor and the risk posed by its processing, the Data Processor ensures the following below indicated technical and organizational measures of data protection. These measures shall be regularly revised and, if needed, updated.

1.2. Technical and organizational data protection measures applied by the Data Processor shall at all time ensure the safety level corresponding to the nature of stored personal data and the risk posed by its processing.

1.3. the Data Processor ensures the security level which corresponds to the level of threat:

1.3.1. the *pseudonymisation* and *encryption* of personal data;

1.3.2. the ability to ensure continuous *confidentiality, integrity, availability* and *resilience of data processing systems and services*;

1.3.3. the *ability to timely restore the availability and access to personal data* in the event of a physical or technical incident;

1.3.4. a *process for regular verification, assessment and effectiveness evaluation of technical and organizational measures* which ensure security of data processing.

1.4. The Data Processor undertakes measures to ensure that no natural person subordinate to the Data Processor, who has access to personal data, processes personal data, except on instructions from the Data Processor.

Organizational and Technical Measures

1.5. <u>Management and control of access to data:</u>

1.5.1. the Data Processor ensures protection, management and control of access to personal data;

1.5.2. access to personal data may be provided only to a person who needs the personal data for execution of his/her functions;

1.5.3. a user can use the personal data to perform only those actions which she/he is authorized to perform;

1.5.4. Requirements for passwords:

- All accounts must have a password expiration.
- Passwords must be changed every 90 days.
- Passwords must be a minimum length of 10 characters.
- Passwords must contain at least the combination of letters, numbers and special characters (!,@,£$§ etc).
- Passwords should not contain employee personal information, which is easily guessed, such as birthdays or names.

- Employees should not set recurring passwords for a minimum of 1 year.
- The same password must not be used for different environments /logins, including employee's personal accounts.
- If the employee needs to store the passwords, encryption must be set. Using a secure password manager is first handedly recommended.
- In the event of leaked passwords, the following steps must be taken:
  report the team leader of compromised passwords
  set new passwords with immediate effect
- Developers must ensure that they always meet the security precautions and industry standards.
- files on computers containing personal data are not accessible to users of other computers;
- data stored on internal servers is divided into separate folders according to the functional purpose and is accessible only to authorized employees;

1.5.5. Access to personal data is controlled with such organizational and technical personal data protection measures which record and control attempts to register and receive rights, i.e. the following logins to personal data are recorded: *logins to the computer, computer network or the database* (login identifier, date, time, duration, login result (successful or failed), *files which have been accessed, actions performed with personal data* (entering, previewing, changing, destroying and other actions).

1.5.6. Records are stored for 3 months.

2. Physical safety

2.1. Physical safety measures:

2.1.1. the security of premises, where personal data is stored, is protected:

2.1.1.1. entrance to premises of the Data Processor (except for open premises intended for client servicing) is possible only with a code, an identification card or by fingerprints;

2.1.1.2. access to premises, where servers are stored, is prohibited for unauthorized persons, whereas restricted, strictly monitored and recorded for authorized persons;

2.1.1.3. premises have a security system installed (alarm);

2.1.1.4. non-employees can access premises only through the reception desk, admitted by authorized persons.

2.2. Copying, recovering and destroying data:

2.2.1. actions of copying or recovering of personal data in case of emergency (when and who has performed the actions) are recorded both automatically (inside the system) and manually (in the Journal of Incidents of the Data Processor). Records are stored for 1 year;

2.2.2. destruction of personal data is recorded (on what basis, when, who and how has destroyed the data by compiling a Personal Data Destruction Act).

2.3. Data reception (provision) security measures:

2.3.1. usage of safe protocols and/or passwords is ensured when personal data is transferred via external data transfer networks;

2.3.2. security control of personal data stored on external data carriers and e-mail is ensures along with deletion of data after usage by transferring it to databases, etc.;

2.3.3. data is received and provided via the Internet (network):

2.3.3.1. data transfer channels are encrypted;

2.3.3.2. login is allowed only from the IP addresses agreed with, set and confirmed by the Data Processor;

2.3.3.3. users are identified by a unique name and password;

2.3.3.4. data is encrypted with a password;

2.3.4. When data is transferred via e-mail, employees shall ensure that:

2.3.4.1. they provide only as much data, as needed for appropriate implementation of work or contractual obligations;

2.3.4.2. the recipient shall process data according to the requirements of the EU;

2.3.5. if the Data Processor must provide personal data under a request from a state institution, the unit of the Data Processor, which has received the request, shall check whether the relevant country institution has the right to require such data. The unit, which has received the request and prepares a response, informs the head of the Data Processor or the authorized person who enters the request for personal data to the registrar of transfer of personal data. The response is registered in the Registrar of Sent Letters;

2.4. Usage and maintenance of computer hardware and software:

2.4.1. protection from malicious software is ensured: all computerized workplaces have antivirus programs installed, working and regularly updated;

2.4.2. it is ensured that system testing is not executed with real personal data, except when it is necessary and when organizational and technical personal data security measures ensuring real security of personal data are used;

2.4.3. computers of the Data Processor are monitored electronically.

2.5. Other (additional) **safety** measures:

2.5.1. personal data stored on active databases is encrypted;

2.5.2. security measures helping to control actions of persons administering the database, server or the computer network are used;

2.5.3. remote units log in to the internal computer network which is protected using the following safety measures: *the unit logs in via the VPN tunnel*;

2.5.4. data protection is ensured by responsible persons and units which do not perform administrative functions;

2.5.5. internal audits on procedures related to provision of access rights are executed;

2.5.6. personal data stored on paper media is processed only in premises of the Data Processor during official working hours of the Data Processor and in compliance with procedures set forth for each position and function, except for transferring data according to signed agreements or legal acts. Employees ensure that all obsolete personal data prints are destroyed in a way that prevents third persons from receiving such personal data.

2.6. Organizational data security measures:

2.6.1. the Data Processor has confirmed written documents regulating data security;

2.6.2. employees are acquainted with documents regulating data security;

2.6.3. documents regulating data security are regularly revised, updated, if needed, and controlled for execution;

2.6.4. responsible employees are **trained** to process data;

2.6.5. employees are prohibited from collecting information about data subjects for their own interests or other purposes which are incompatible with direct orders related to data processing;

2.6.6. employees sign **non-disclosure agreements** which oblige the employee to refrain from using information received from the employer or in relation to performed work functions, which is defined as confidential in the non-disclosure agreement, for personal or commercial purposes during execution and after expiration of the employment agreement;

2.6.7. employees confirm that they are acknowledged with the present measures with signatures;

2.6.8. when it turns out that the employment agreement is terminated or the employee is transferred to another work position or a unit or a department, or the employee leaves the Data Processor for a long period of time, responsible persons remove or limit or change or suspend access rights of the employee to systems, resources, tools, email and/or work instruments used in the Data Processor and/or perform other actions.

Signatures of the Parties:

On behalf of Controller Riigi Kaitseinvesteeringute Keskus Ivar Janson */signed digitally/*	On behalf of Processor Stebby OÜ Karl-Eduard Möldre */signed digitally/*