PRIVACY POLICY

This privacy policy ("**the privacy policy**") describes how Muusa Majutus OÜ ("**the company**") processes the personal data of its employees, customers or people who engage in cooperation with the company in any other manner and which measures we apply for protecting personal data.

Personal data are processed pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) and other national and European privacy legislation and regulations (together "**the data protection law**").

The definitions used in this privacy policy are set out on page 2.

1. SCOPE

This privacy policy applies to all the personal data that we process as a controller.

The company processes personal data of its employees, temporary employees, sole proprietors, applicants for jobs and positions, suppliers' contact persons, customers, visitors and other partners.

2. PURPOSE

The purpose of this privacy policy is to explain which personal data we process and how and why we do that. In addition, this privacy policy outlines our obligations and liability upon protecting data.

This privacy policy is not an exhaustive statement of our data protection practices in various fields, such as security. More detailed rules and instructions will be provided of which we will also inform you at the internal level to the extent practicable.

DEFINITIONS

Whenever used in this privacy policy, the following definitions will have the following meanings:

EEA means the European Economic Area.

GDPR means the EU General Data Protection Regulation ((EU) 2016/679) the implementation of which starts on 25 May 2018.

Personal data means any data and information that are related to a natural person, i.e. an individual, and that make it possible to establish the identity of the individual. The identity of an individual can be established if the individual can be identified on the basis of the data without any disproportionate effort and within a reasonable scope. The basis for identification may be a name, a personal identification code, location data, an online identifier or a physical, physiological, genetic, mental, economic, cultural or social identity or a combination of thereof.

Special categories of personal data means personal data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,

as well as genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Customer means a natural person to whom the company provides services and/or offers goods in connection with its economic activities.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Partner means a natural person who is a supplier of the company or an employee/representative/contact person of another partner who is a legal person.

Visitor's card information means the following data about a visitor to an accommodation establishment as required in the Tourism Act: the name, date of birth, citizenship and address; the name, date of birth and citizenship of the spouse and a minor accommodated with the visitor; the period of provision of the accommodation service; if the person is not a citizen of Estonia, an EEA Member State or Switzerland or an alien residing in Estonia on the basis of a residence permit or right of residence, then also the type and number of the travel document and the state that issued it.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Processing means any operation or set of operations that is performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing may take place manually or by using automated systems, such as IT systems.

Contractor means a natural person (i.e. not a company) with whom the company has entered into a contract for services (contract for the provision of services), including also members of the management bodies of the company.

Controller means the person who decides why and how (i.e. for which purposes and in which manners) personal data are processed. The following questions may be of help when determining the controller.

- Who decides which personal data are stored?
- Who decides for which purposes personal data are used?
- Who decides in which manner personal data are processed?

If a person themselves decides on processing the personal data in their possession and is liable for the data, this means that the person is a controller.

Processor means a person who processes personal data on behalf of the controller. If personal data are in the possession of a person or a person processes the data, but the

person has no power to decide on the processing thereof, i.e. the person processes the data by following the instructions issued by the controller, this means that the person is a processor. A processor may be a service provider (for example, the person who provides payroll accounting service).

1. CATEGORIES OF PERSONAL DATA

1.1 Employees and contractors

The company processes personal data of its employees, applicants for jobs and positions (for example, members of the management board) and contractors as well as former employees and former contractors.

These personal data include the following:

- personal details, such as name, date of birth, bank account details, close relatives, details of social media accounts, visa/passport/ID card data or a copy of a respective document;
- contact details, such as address and telephone number, email address;
- personnel file details, including: terms and conditions of the employment relationship, training, performance evaluations, promotions, personal development plans, conduct and disciplinary data, work location, salary information, bank account details, tax number and personal identification code;
- employment history / application details, such as educational history and employment history;
- family details, such as names and dates of birth of children (these are relevant if a person is applying for parental leave);
- details regarding trade union membership;
- performance related data, such as annual salary reviews of employees, psychometric testing, etc.;
- special categories of personal data: medical details, such as medical certificates and certificates for sick leave.

The above list is not exhaustive, but covers the most commonly collected, used and otherwise processed personal data.

1.2 Customers

The company also processes personal data of its customers. These personal data may include the following:

- personal details, such as name, date of birth / personal identification code;
- contact details, such as address and telephone number, email address;
- visitor's card information.

1.3 Partners

The company processes personal data of its partners. Such personal data may include the following:

- personal details, such as name, title, position, work identification numbers, department, business unit (including contact data collected for training/verification);

- contact details, such as email address, telephone numbers and work location;
- tax details, such as VAT/tax numbers.

2. PURPOSES OF PROCESSING

The company processes personal data for the purposes for which the personal data have been collected.

We process personal data of our employees for example for the following purposes:
- performance of the employer's obligations provided for the company in the Employment Contracts Act;
- payroll and benefit administration;
- HR, performance and talent management;
- internal audits.

We process personal data of our customers and partners for example for the following reasons:
- performance of the obligations of an accommodation establishment provided for in the Tourism Act (for example, completing a visitor's card and storing it for a period of two years);
- preparation and performance of a contract entered into with the customer/partner;
- marketing and public relations;
- improvement of products and services of the company;
- research and statistical analysis;
- development of the business strategy of the company;
- prevention and detection of unlawful and/or criminal behaviour towards the company or our customers and employees.

We may also process personal data for other reasons from time to time. The company tries to ensure that individuals are informed about the purposes of processing their personal data at the time the company receives the personal data. Where this is not possible or practicable, we try to inform individuals as soon as possible after receiving the personal data or processing thereof in any other manner.

3. PROFILING

The company engages in profiling various individuals (for example, employees, contractors, applicants for jobs or positions as well as customers). The company engages in the following type of profiling:
- *for the evaluation of workforce;*
- *for analysing presence and performance;*
- *for analysing customer preferences.*

The company engages in processing such data if: a) this is expressly authorised by law; b) this is necessary for entry into or performance of a contract; or c) the individual has given appropriate consent.

If you make automated decisions, including profiling, we notify individuals of the logic used and of the importance of the processing and forecast results thereof for the data subject.

4. RIGHTS OF DATA SUBJECT

Individuals have certain rights relating to their personal data under the data protection law.

4.1 *Right of access* – you have the right to know what data are stored about you and how they are processed.
4.2 *Right to rectification* – you have the right to request the rectification of your personal data if they are incorrect.
4.3 *Right to erasure ('right to be forgotten')* - in certain cases you have the right to request your personal data be erased (for example, if we no longer need them or you withdraw your consent for processing the data, etc.).
4.4 *Right to restriction of processing* – in certain cases you have the right to prohibit or restrict the processing of your personal data for a specific period (for example, when you have objected to the processing of data).
4.5 *Right to object* – on grounds relating to your particular situation, you have the right to object to the processing of your personal data when processing is based on our legitimate interest or in the public interest. If personal data are processed with the purpose of direct marketing, objections may be filed at any time.
4.6 *Right to data portability* – If processing of personal data is based on an individual's consent or a contract entered into with the company and the processing of the data is carried out by automated means, the individual has the right to receive the personal data concerning them, which the individual has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller. The individual also has the right to demand that the company transmit the personal data directly to another controller, *where technically feasible*.

4.7 *Automated decision-making (including profiling)* – in a situation where we have notified you that we are making decisions based solely on automated processing (including profiling), which produces legal effects concerning you or significantly affects you, you may demand that decisions not be made solely on the basis of automated processing.

The data subjects rights and requests procedure explains how the requests related to the abovementioned rights can be submitted and how the company will manage such requests.

5. SECURITY

5.1 Security measures

The company has physical, technical and organisational measures in place to protect personal data from unlawful or unauthorised destruction, loss, change, disclosure, acquisition or access.

The company uses the following physical data security measures:
- documents on paper, which contain personal data, are held in locked premises and filing cabinets to which only certain employees have access for performing their duties of employment;
- data processing premises and IT systems are sufficiently protected against fire, overheating, water, power fluctuations and power cuts.

Technical security measures used in the company include the following:
- video surveillance;
- all office computers are protected with a screen saver provided with a password when an employee leaves work;

- it is ensured that the IT system does not allow any new attempts to enter and will lock the user ID if the number of failed attempts to enter exceeds a certain limit;
- it is ensured that especially vulnerable systems (e.g. laptops, smart phones) are sufficiently well protected (by using, for example, encrypting or other manners).

Organisational security measures that we use are the following:

- accesses to important IT systems and premises are regulated;
- roles and profiles have been assigned to all users of IT systems;
- it has been determined which users may access which data and the access rights correspond to the needs arising from the employee's duties of employment;
- it is ensured that access rights are annulled when the employee leaves the company;
- no unauthorised access from public premises to premises that are used for processing personal data is ensured;
- visiting procedure has been drawn up for visitors to the company (i.e. for visitors to non-public premises) and the visitors' data as well as the times of their arrival and departure are registered when they arrive and leave the company;
- the premises where the computers that allow access to the IT system are located and the premises where the documents that contain personal data are held are also under inspection/surveillance after the end of the working time.

5.2 Personal data breaches

The company will deal with personal data breaches in accordance with the provisions of the personal data breach response procedure. Instructions for the establishment of personal data breaches and notification thereof can be found in the personal data breach response procedure.

6. DISCLOSURE OF PERSONAL DATA

From time to time, the company may disclose personal data to third parties or allow third parties to access the personal data that we process (for example where a law enforcement authority or the Estonian Data Protection Inspectorate submits a valid request for access to personal data).

The company may also share personal data: a) with another person belonging to the same group with the company (for example, the parent company and subsidiaries, the ultimate beneficial owner of the group and its subsidiaries); b) with selected third parties, including business partners, suppliers and contractors; c) with other third parties when we sell or buy other companies or assets (i.e. upon concluding transactions); or d) if the company is under a legal obligation to disclose personal data (this includes exchanging information with other companies and organisations for the purposes of fraud prevention).

Where the company enters into contracts with third parties to process personal data on behalf of the company, it will ensure that the appropriate contractual protections are in place to safeguard the personal data, using, among other things, the data protection standard clauses that have been developed for embedding in the contracts to be entered into with persons who process data on behalf of the company.

The company discloses personal data or grants them access to the following categories of persons for the purposes explained below:

- providers of communications services – for organising call and data communications services of employees;

- payroll accounting service providers – for keeping payroll accounting of employees;
- providers of occupational health service – for organising occupational health of employees;
- recruitment agencies – for finding new employees/contractors;
- marketing companies – for doing direct marketing to the customers specified by the company;
- insurance intermediaries and insurers – for providing employees of the company with travel, accident or another similar insurance.

7. STORAGE OF DATA

The company stores personal data only for as long as the storage of such personal data is deemed necessary for the purposes for which the personal data were collected. Personal data are stored in accordance with relevant laws and company guidelines.

The company adheres to the following criteria upon storage of personal data:

- we store personal data as long as it is necessary in order to provide our services;

- if a person has a customer account or a customer card at the company, we will store their personal data for as long as the account/card is valid or for as long as such data are needed to provide services to them;

- if the company has a statutory, contractual or similar obligation to store personal data, we will store the personal data as long as it is necessary to perform such an obligation;

- after the termination of a contractual relationship, we will store certain data for as long as the person (data subject) or the company itself has the right to file claims against the other party under the contract.

Some examples:

- Pursuant to the requirements of the Tourism Act, we store visitor's card information for two years as of the date the card was completed.

- Pursuant to the requirements of the Employment Contracts Act, we store written documents of employment contracts for ten years as of the date of expiry or termination of the employment contract.

More detailed criteria are provided for in *the register of personal data* of the company.

8. RESPONSIBILITIES

The company is responsible for the processing of personal data. The management of the company has overall responsibility for the compliance of the company with this privacy policy and will designate a primary point of contact in relation to i) the processing of personal data of the employees and contractors of the company; ii) the processing of persona data of customers and partners; and iii) the security of the personal data processed by the company.

All employees of the company who are engaged in the processing of personal data must comply with the most up-to-date version of this privacy policy as published from time to time.

9. ASSOCIATED POLICIES AND PROCEDURES

This policy should be read in conjunction with the following policies and procedures:

- Personal data breach response procedure;
- Data protection standard clauses for data processing contracts;
- Data subjects rights and requests procedure;
- Privacy notice (to employees, customers);
- Register of personal data.

Date: 9 May 2018