**PRIVACY POLICY**

In the current Privacy Policy (the “**Privacy Policy**”) we describe how [company name] (the “**company**”) processes the personal data of its employees, clients or other persons who cooperate with the company, and what means we utilise to protect this personal data.

The personal data is processed according to the General Data Protection Regulation (Regulation (EU) 2016/679), as well as the other domestic and European privacy laws and regulations (jointly the “**data protection legislation**”).

The terms used in this Privacy Policy are defined on the second page.

**1. SCOPE**

The current Privacy Policy applies to all of the personal data we process as a controller.

Examples of the individuals whose personal data the company processes include the company’s employees, temporary employees, self-employed persons, work and job position candidates, supplier contact persons, clients, visitors and other cooperation partners.

**2. AIM**

The aim of the current Privacy Policy is to explain what types of personal data we process, as well as to show why we process this data. The Privacy Policy further describes our obligations and responsibilities with regard to data protection.

The Privacy Policy does not describe our data protection activities completely. There are more precise regulations and manuals available in different fields, for example, “security”, which we will inform the employees of the company about internally, to a reasonable extent.

**TERMS**

The current Privacy Policy uses the following terms, with the following meanings:

**EEA** – European Economic Area (the currently valid regulation indicates that the EEA consists of all European Union member states, as well as Norway, Iceland and Liechtenstein).

**GDPR** – this is the EU General Data Protection Regulation (EU) 2016/679), the implementation of which began on 25 May 2018.

**Personal data** – this includes all the kinds of data and information which are connected with a physical person or a human, which permit that person’s identity to be determined. A person is identifiable if, without disproportionate effort, the data permits the identity to be established on a reasonable basis. Identifiable characteristics include, singly or jointly, the person’s name, identity code, location information, network indicator or physical, physiological, genetic, mental, economic, cultural and social characteristics.

**Personal data special categories** – this is the personal data which establish a person’s racial or ethnic background, political views, religious or philosophical beliefs or union membership, as well as the genetic data and biometric data used for the unique identification of a person, health data or data about a person’s sexual life or sexual orientation.

**Personal data related violations** – these are security breaches that result in personal data that is forwardable, saveable or processable by other means being unwillingly or illegally destroyed, lost, changed, publicised or accessed in an unauthorised manner.

**Client** – this is a physical person to whom the company provides services and/or offers goods through its economic activities.

**Third party** – this is a physical or legal person, public sector institution, agency or an entity, except a data subject, controller or an authorised processor, and the persons who may process personal data as the direct subordinates of the controllers or authorised processors.

**Cooperation partner** – this is a physical person that is a supplier to the company or is the employee / representative / contact person for another legal person in a cooperation partnership.

**Guest registration card data** – the data required by the tourism legislation concerning the visitor to a place of accommodation including the name, date of birth, citizenship and address; name, date of birth and citizenship of the accompanying spouse and underage children; accommodation dates; and for citizens outside of Estonia, the EEA or Switzerland, or for foreigners in Estonia with a residency permit or residency rights, the type and number of the travel document and its issuing country.

**Profile analysis** – this is any kind of automated personal data processing, which includes using the personal data for the purpose of evaluating personal aspects known to be associated with a physical person, foremost for the analysis and prognosis of such aspects which are related to the work results of the relevant physical person, as well as the economic condition, health, personal preferences, interests, trustworthiness, behaviour, location or mobility.

**Processing** – this is an activity, or a collection of activities, performed with the personal data such as collecting, documentation, ordering, structuring, storing, adjusting and changing, making enquiries, reading, using, forwarding, distributing or publicising the data through making it otherwise accessible, unifying or joining, restricting, erasing or destroying the data. Such processing may take place by hand or through automated systems such as IT systems.

**Contractor** – this is a physical person (not a company), with whom the company has signed a service contract (service provision contract) including the members of the management body of that company.

**Controller** – this is the person who decides why and how (the aims and methods) the personal data is processed. Answering the following questions may help to determine the controller:

- Who decides what items of personal data are stored?

- Who decides for the aims for which the personal data will be used?

- Who decides how the personal data will be processed?

The person who decides on the processing of the personal data, which is accessible to himself/herself, and is responsible for the data, is the controller.

**Authorised processor** – this is the person who processes the personal data on behalf of the controller. If this person possesses the personal data or processing it, but does not have the authority to decide how the data is processed, meaning that the processing takes place according to the controller’s instructions, then this person is an authorised processor. The authorised processor may also be a service provider (for example, a payroll service provider).

**1. PERSONAL DATA CATEGORIES**

**1.1 Employees and contractors**

The company processes the personal data of its employees, job and office candidates (e.g. board members) and contractors, as well as former employee and contractor data.

The personal data that is processed includes:

* Personal data such as a person’s name, date of birth, bank account-related data, close relatives, social media account data, visa / passport / ID card data or a copy of the appropriate document;
* Contact data, such as a person’s address, phone number and e-mail address;
* Personal file data including: work relation conditions, training data, work result evaluations, promotions, personal development plans, behavioural and disciplinary data, work location, salary data, bank account data, as well as a person’s taxpayer number and identity code;
* Work relation history / candidacy data – for example, a person’s education and former employment history;
* Family member data – for example, the names and dates of birth of a person’s children (this data is relevant when, for example, the person applies for parental leave);
* Labour union membership data;
* Work achievement-related data – for example, an employee’s annual salary review, psychometrical testing results, etc.
* [*If required, change and amend the above*]
* Special categories of personal data: health data such as medical certificates and sick leave certificates;

[*What other special categories of personal data do you process in the case of employees?*]

The above list is not complete, but it covers the most frequently collected, used or otherwise processed categories of personal data.

**1.2 Clients**

The company also processes the personal data of its clients. The client personal data may include the following:

* Personal data such as a person’s name, date of birth / identity code;
* Contact data – for example, a person’s address, telephone number and e-mail address;
* Guest registration card data;
* Credit card data such as the card number expiry date and CVV number;
* Personal preferences data such as […].
* [*If required, change and amend the above.*]
* Special categories of personal data: [*Name the data special categories of personal data you process with regard to clients.*]

**1.3 Cooperation Partners**

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

* Personal data – for example, a person’s name, job position, work-specific identification numbers, department, business unit (incl. training/evaluation reports and relevant contact data);
* Contact data – for example, a person’s e-mail address, telephone number and work location;
* Taxation data – for example, a person’s valued added tax identification / taxpayer number.
* [*If required, change and amend the above.*]

**2. AIMS OF DATA PROCESSING**

The company processes personal data according to the aims for which the personal data was collected.

For example, the employee personal data is processed with the following aims:

* Fulfilment of the obligations stipulated in the employee’s contract;
* Salary and compensation management;
* Management of personnel activities, performance and talent;
* Internal audits.
* [*If required, change and amend the above.*]

The personal data of clients and cooperation partners is processed, for example, for the following reasons:

* The fulfilment of the tourism legislation stipulated the obligation to name the accommodation place (e.g. the completion of guest registration cards and their storage for 2 years;
* Preparation and fulfilment of a contract signed with a client / cooperation partner;
* Marketing and public relations;
* Development of the company’s product and services;
* Research and statistical analysis;
* Development of the company’s business strategy;
* Avoiding and discovering unlawful and/or criminal behaviour involving the company or our clients and employees.
* [*If required, change and amend the above.*]

Occasionally, we may process personal data for other reasons. The company tries to ensure that the people concerned are informed of the data processing aims at the time of the data collection. We will endeavour to inform people at the first opportunity, after receiving the personal data or before it is processed for other reasons, if it was not possible or sensible to inform the people concerned at the time of the data collection.

**3. PROFILE ANALYSIS**

The company performs a profile analysis of different people (e.g. its employees, contractors, job and office candidates, as well as its clients). The company performs the following types of profile analyses:

* [*Examples: talent management and worker evaluations;*
* *Presence and performance analyses;*
* *Client preference analyses*]

The company processes such data: a) which is explicitly permitted by law; b) which is required or necessary for the signing and fulfilling of a contract; or c) for which a person has given the required agreement.

We inform people of the logic that is used, the importance of such processing and the predicted results for the data subject in the case of automated decisions including a profile analysis.

**4. DATA SUBJECT’S RIGHTS**

People have certain rights in connection with their personal data, according to the data protection legislation.

*4.1. Right to data access* – you have the right to know what data we hold concerning you, and how that data is processed.

*4.2. Right to data rectification –* you have the right to demand corrections to your personal data, in cases where it is inaccurate.

*4.3. Right to data erasure (“right to be forgotten“)* – you have the right, under certain conditions, to request that we erase your personal data (e.g. if we no longer need the data, if you revoke the agreement giving us the right to process the data, etc.).

*4.4. Right to restrict data processing* – You have the right, under certain circumstances, to forbid or restrict the processing of your personal data for a certain period (e.g. if you have submitted an objection concerning the data processing).

*4.5. Right to present objections* – you have the right to present objections concerning the processing of your personal data, considering the concrete situation, if the data processing is taking place according to our legitimate interests or the interests of the general public. Objections to the processing of data for direct marketing purposes can be made at any time.

*4.6 Right to data portability* –in cases where the personal data processing is based on your agreement or a contract signed with us, and the data is processed automatically, you have the right to access the data concerning yourself, which you have given to our controller, in a structured, generally usable format as well as in a machine-readable format for the purpose of forwarding to another controller. You may also request that the company forward the data directly to the other controller, *if this is technically possible*.

*4.7. Automatic decision-making (incl. profile analysis)* – you may demand that a decision is not made based solely on automatic processing, if we have informed you that we used decision-making (incl. a profile analysis) based on automatic processing which has resulted in legal consequences concerning yourself.

The Data Subject Rights and Application Procedure explain how applications can be presented with regard to the abovementioned rights, and how the company manages such applications.

**5. SECURITY**

**5.1 Security Means**

The company has established physical, technical and organisational means to protect the personal data against its unlawful or unauthorised destruction, loss, manipulation, publication, possession or access.

For example, the company uses the following physical means of data protection:

* Paper based documents containing personal data are stored in locked rooms and cabinets, to which only certain employees have access for the purpose of fulfilling their job assignments;
* Data processing rooms and IT systems are sufficiently protected against fire, overheating, water, current fluctuations and power outages.
* [*If required, change and amend the above.*]

The technical security means used by the company include, for example:

* Video surveillance;
* All work computers are protected with password-protected screensavers when the employee leaves;
* Ensuring that the IT systems do not permit new entry attempts and that the username is locked if a certain number of unsuccessful attempts have been made;
* Ensuring that especially vulnerable systems (e.g. laptops, smartphones) are sufficiently protected (using encryption or other means).
* [*if required change and amend the above*]

We use organisational security measures:

* Which control access to the important IT systems and rooms;
* According to which, all users of the IT system have assigned roles and profiles;
* Which determine the data that can be accessed by which users, and ensure that the access rights correspond with the employee’s work duties;
* Which ensure that the access rights are deleted when an employee leaves the company;
* Which ensure that it is not possible to access rooms where the data is processed from public areas, without prior authorisation;
* According to which company visitors (meaning visitors to the rooms that are not in public use) must have a visiting order and the visitor’s data, arrival and departure time is registered upon their arrival and departure;
* Which mean that the rooms with access to the IT system computers and the rooms containing documents with personal data are controlled / under surveillance outside of office hours.
* [*If required, change and amend the above.*]

**5.2 Violations in relation to personal data**

The company reacts to violations in relation to personal data according to the procedures established concerning personal data violations. Instructions for identifying and informing the persons concerned about the personal data violations are found in the Personal Data Violation Reaction Procedure.

**6. PUBLICATION OF PERSONAL DATA**

The company may occasionally release personal data to third parties, or provide access to the personal data processed in the company (for example, when the law enforcement authority or the Data Protection Inspectorate presents a valid demand for the accessing of personal data).

The company may also share personal data: a) with a person in another company within the same group (e.g. a parent and subsidiary company, or the group’s end beneficiary and its subsidiary companies); b) with selected other parties incl. business partners, suppliers and contractors; c) with other parties when selling or buying other companies and assets (incl. while making transactions); or d) when the company has a legal obligation to release the personal data (which includes information exchanges with other companies and organisations for the purpose of avoiding fraud).

When the company signs agreements with other parties for the processing of personal data on behalf of the company, then the company shall ensure that the appropriate contractual protection means are in place for the protection of the personal data used by others, or the Data Protection Standard Clauses, which have been developed for the purpose of adding to contracts which are signed with the persons processing data on behalf of the company.

The company may release personal data or grant access to the data to the following categories of people, for the reasons explained below:

* Communication services providers – employee contact and data communication organisations;
* Payroll service providers – for the monitoring of employee salaries;
* Occupational health service providers – for organising the occupational health of employees;
* Recruitment agencies – for finding new employees / contractors;
* Marketing companies – for sending direct marketing to the clients specified by the company;
* Insurance brokers and insurers – for providing the company employees with travel, accident or other forms of insurance.
* [*If required, change and amend the above.*]

**7. DATA STORAGE**

The company stores personal data only for as long as the preserving of the personal data is deemed necessary to fulfil the aims for which the personal data was collected. The personal data is stored according to the relevant legislation and company principles.

The company shall consider the following criteria when storing personal data:

* How long the personal data must be kept in order to offer the company’s services.
* If the person has a client account or a loyalty card, then the personal data will be stored for as long as the account / card is active or for as long as is required in order to offer personalised services.
* When the company has a legal, contractual or other similar obligation for storing the personal data, then the data will be stored for as long as is required to fulfil such an obligation.
* After the end of the contractual relations, certain data will be stored for as long as the person (data subject) or the company itself has the right to present demands to the other party based on a contract.

Some examples include:

* Guest registration cards are stored for 2 years, from the moment when the card is filled in according to the requirements of the tourism legislation.
* Work contract written documents are stored for a period of 10 years after the work contract has ended, according to the requirements of the Employment Contracts Act.
* Credit card data is stored until the accommodation services have been provided in an orderly fashion, according to the contract. [If there is a need to store credit card data for a longer period, than explain why and for how long.]

More precise criteria are specified in the company’s *Personal Data Register*.

**8. DATA FORWARDING OUTSIDE THE EEA**

The company may sometimes need to forward personal data outside the EEA. Such forwarding takes place according to the valid data protection legislation[[1]](#footnote-1). The company utilises reasonable measures to ensure that the personal data transferred outside the EEA is treated securely and according to its Privacy Policy.

The company forwards personal data to the following locations outside the EEA for the reasons mentioned below, using the following means for the protection of the personal data:

* [*Country to which the data is forwarded – aim of the forwarding – security description.*]

[As an explanation, the security may be e.g. binding group internal rules, standard data protection clauses as accepted by the European Commission, etc. (see the GDPR Art. 46-49).]

**9. AREAS OF RESPONSIBILITY**

The company is responsible for processing personal data. The general responsibility for following the stated Privacy Policy in the company rests with the company management, which shall assign a chief contact in connection with: i) the processing of the personal data of company employees and contractors; ii) the processing of the personal data of clients and cooperation partners; and iii) the security of the personal data processed in the company.

All company employees who are in contact with the personal data for the processing purposes are obligated to follow the most current issue of this Privacy Policy.

**10. RELATED REGULATIONS AND PROCEDURES**

The Privacy Policy must be read together with the following rules and procedures:

Personal Data Violation Reaction Procedure

* Data Protection Standard Clauses for data processing contracts
* Data Subject Rights and Application Procedure
* Privacy Policy (employees, clients)
* Personal Data Register
* [*Amend if you have, or will establish, additional regulations.*]

Date: […]

1. The GDPR Articles 45-49 stipulate when, and under what conditions, the forwarding of data is permitted. GDPR Article 45 stipulates that personal data may be forwarded outside the EU when the European Commission has made a decision that such a third country, territory or international organisation will ensure a sufficient level of protection for the personal data. Such forwarding does not require special permission. The relevant countries, territories and International organisations are publicised in the *Official Journal of the European Union* and on the commission’s website. [↑](#footnote-ref-1)