Happenee s.r.o.

INFORMATION SECURITY AND PERSONAL DATA POLICY

The company Happenee Ltd., ID: 04216202, registered office Baštýřská 142, Hostavice, 198 00 Praha 9 (hereinafter "Happenee") supports the creation and continuous development of information security management system, so as to protect assets and to its employees, customers and partners to provide adequate degree of certainty.

For this reason, Happenee's top management approves and promotes this Happenee information and personal data security policy as a framework for the company's direction in the field of information security protection. The intention of the management is to support the set goals and principles of this policy.

The established security policy is proportionate to the intentions of Happenee, and includes information security objectives for personal data, taking into account the basic conceptual requirements imposed in particular in the internationally recognized ISO / IEC 27002 standard and the related ISO / IEC 2700X standard. These internationally recognized guidelines define the requirements for an information security management system.

The information security policy for personal data, communicated throughout the organizational structure, is available as documented information and is reasonably available to interested third parties.

With this policy, Happenee declares to all business partners, employees, public and state administration and the general public the ability to effectively protect information, tangible and intangible assets owned and entrusted in accordance with legislative requirements with applicable legislation of the Czech Republic and the European Union, international agreements and other protection requirements on information security.

For the purposes of this Happenee Information Security Policy, the following are defined:

- "assets" means Happenee's personal data;
- "Happenee" the company Happenee Ltd., ID: 04216202, registered office Baštýřská 142, Hostavice, 198 00 Praha 9; entered in the Commercial Register kept at the Municipal Court in Prague, Section C, Insert 19069;
- "incident" means a detected occurrence of a system state, service state, or network state indicating a possible breach of information security policy or failure of action, and more;
- "Civil Code" or "Trademark Code" means Act No. 89/2012 Coll., The Civil Code;
- "personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is a natural person who can be identified, directly or indirectly, in particular by reference to a specific identifier, such as name, identification

number, location data, network identifier or one or more specific physical, physiological, genetic, mental, economic, cultural or the social identity of that natural person;

● “processing agent” means a person authorized by Happenee who processes or has access to personal data on the basis of an employment contract, a service contract, an out-of-employment agreement or other contracts or agreements concluded with Happenee in the performance of his or her duties;

● “person with authorization” means a person authorized to process Happenee personal data with special access defined by a username / designation, based on an instruction, performance of a contract or other fact that has been assigned a username / designation by which he or she is granted special access to personal data;

● "Happenee Platforms" means all platforms that Happenee manages, owns, directs, develops or participates in their operation, including the Happenee Platform, which is used to organize social, sporting, cultural or other events;

● “Security Policy” means this Happenee Privacy Policy on Personal Data;

● "storage", or the server is the central place where data is stored and maintained;

● “Labor Code” or “ZP” means Act No. 262/2006 Coll., The Labor Code;

● "processor", "data", "personal data" and "processing" have the same meaning as ascribed to them by GDPR.

● Other terms used in this contract have the same meaning as ascribed to them by the ISO / IEC 27000 standard.

Definition of Happenee assets

Happenee's assets consist of all personal data relating to Happenee employees, personal data of Happenee business partners, personal data obtained from customers as part of the provision of services by Happenee and users of Happenee platforms. Based on contractual relationships with employees, customers and business partners, Happenee is entitled to have access to and process their personal data in accordance with the high standards of personal data protection, which are the subject of this Security Policy, among others.

Happenee processes personal data mainly in the following activities:

● Operation of Happenee platforms

● Monitoring of customers and users of Happenee platforms via logs

● When providing services to Happenee customers and business partners

● Archiving of contractual documentation

Happenee's privacy policy is set out in the following sections of this document. The individual points contain information concerning organizational security measures, assigned functions / roles and related responsibilities, managing access control to systems and applications, managing assets and ensuring the confidentiality of employees and other persons and others.

1. Organizational and security measures

Personal data should be processed in such a way as to guarantee the appropriate security and confidentiality of such data, inter alia in order to prevent unauthorized access to personal data and to the equipment used for their processing or unauthorized use.

Happenee ensures that the personal data of data subjects are processed fairly and in a lawful and transparent manner. Further ensures that the personal data of data subjects are collected for specific, explicit and legitimate purposes and to prevent their processing in a way that is incompatible with those purposes.

When processing personal data of data subjects, Happenee shall ensure that personal data are proportionate, relevant and limited to the extent necessary in relation to the purpose for which they are processed.

Happenee is aware that the personal data processed by data subjects must be accurate and, where necessary, updated, all reasonable steps must be taken to ensure that personal data which are inaccurate, taking into account the purposes for which they are processed, are deleted or rectified without delay, furthermore, personal data must be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.

Happenee takes technical and organizational measures, taking into account the nature, scope and purposes of the processing, to ensure that the processing of personal data complies with the Regulation.

a) Security of human resources

The processing agents understand their obligations. When selecting an employee for Happenee, each candidate is screened in accordance with applicable law, i.e. in particular the Labour Code, the Civil Code and in accordance with ethics.

Recruitment is an internal procedure, taking into account Happenee's usual practice, which results in the selection of the most suitable candidate, subject to strict criteria and the high standard required of all staff. Before starting work, each candidate is:

- acquainted with Happenee's internal procedures and recommendations. Each person in charge of processing is required to follow these procedures and recommendations established throughout Happenee, in accordance with this security policy.

During the processing of Happenee personal data, the person thus entrusted has the obligation in particular:

- store all information and data on the company server / storage;
- use only assigned work aids to transfer this data;
- not download data from the server / storage to other fixed storages, unless otherwise agreed with the customer, such an agreement must then be confirmed in writing, at least in e-mail communication;
- not to store data outside the company server / storage, unless otherwise agreed with the customer, such an agreement must then be confirmed in writing, at least in email communication;

In the event of a change in the job position, job description or content of the function assigned to the person authorized to process, the scope of access to the personal data of such authorized person will be updated. Each person authorized to process such a fact shall be required in particular to:

- immediately inform your supervisor if he or she finds that there has been an incorrect form of updating access to personal data;
- not to actively search for, download, use or disclose this data in any way;
- inform your supervisor immediately if he or she finds that he or she has other access to the data;

Any person authorized to process will be denied access to Happenee's personal data after termination of employment, termination of the service contract or other similar means of termination of cooperation with Happenee. The person authorized to process before the termination of the contractual obligation with Happenee in particular:

- will notify Happenee immediately if he or she determines that he or she still has any access to the data
- submits the assigned work aids on the basis of the output form

What happens to a person's access in the event of termination of employment / termination of services:

- on the day of termination of work, or a similar contractual relationship, the account of the authorized person is cancelled
- by cancelling the account in itself, this person automatically loses access to all other tools, as they are linked to this user account

In the event that the person responsible for processing violates the obligations set out throughout the Happenee, in particular in this security policy, as well as other obligations imposed by Happenee instructions, orders and recommendations, a classification of basic offenses and associated sanctions is established.

- in the event of a minor breach of information security, a complaint will be imposed on the person concerned
- in the event of a moderate information security error, the person concerned will be required to confront Happenee's management and will be retrained
- in the event of a gross error in the security of information, the person concerned will be terminated at work, or similar relationship

b) Physical and environmental security

When processing its assets, Happenee takes care to ensure the security of the space and environment where personal data is processed. Each person in charge of processing follows the procedures and mechanisms set out by Happenee.

The physical security of workers' offices is ensured through the lockable doors of such offices, and only authorized persons have access to them.

Happenee follows the principles of the so-called empty table and blank monitor screen. These principles are intended in particular to ensure that personal data recorded in paper form are not freely located on office premises, but that such paper documents are securely stored in premises with secure and limited access.

In addition, Happenee ensures that computers and other terminals are left with logged-off persons with authorization or protected by a mechanism that locks the screen or keyboard.

Happenee devices that process (store) personal Happenee data are located and protected to reduce the risk of threats and dangers.

Happenee has procedures in place for the safe disposal of equipment, including the removal of personal data stored on it.

c) Network Security Management

Happenee, through authorized persons, ensures the protection of information in networks and their support means for information processing, at the same time it is aware of the need to separate the group of information services, authorized persons and information systems in individual networks.

The company also introduces security mechanisms for network services, operating procedures and measures to protect information against malware, information backup procedures, controlled installation procedures and regular software updates on operating systems, including the introduction of communication encryption using a security HTTPS certificate.

Happenee also ensures maximum information security through the OWASP community to which it subscribes. OWASP is a community dedicated to web application security.

d) Transmission of information

Happenee takes care of the security of information when it is transmitted within the organization and with external entities. Protection applies to assets transferred electronically and physically.

Persons authorized to process, outside the scope of the powers conferred on them within the assigned function / role, may not in any way handle and manipulate Happenee personal data without the consent of the person responsible for compliance with the security policy.

e) Security incidents

One of the requirements under Article 5 (1) (a) f) The Regulation is that, when appropriate technical and organizational measures are taken, personal data are processed in a way that ensures adequate security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage.

According to the Regulation, the term "destruction" is interpreted as a case where the data no longer exists at all or at least not in a form to be useful.

The term "damage" is interpreted as the case where personal data are altered or no longer complete.

The "loss" of personal data is interpreted as meaning that the data may still exist, but Happenee has lost control or access to it or no longer holds it.

Unauthorized or unlawful processing under the Regulation includes disclosure of personal data to recipients (or their access) who are not authorized to obtain (or have access to) the data or any other form of processing that is in breach of the Regulation.

For this reason, Happenee, as the controller, ensures that it has the appropriate technical and organizational measures in place to ensure a level of security commensurate with the risk that accompanies the processing of personal data.

Furthermore, Happenee takes into account the current state of development, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of variable probability and relevance to the rights and freedoms of individuals.

Happenee is aware of the above requirement, including the requirement that personal data breaches be reported to the relevant national supervisory authority and, in certain cases, that personal data breaches be disclosed to individuals whose personal data have been affected.

Therefore, Happenee plans and implements procedures in advance to detect and manage a breach without delay, assess the risk to individuals and then determine whether it is necessary to notify the relevant supervisory authority and, where appropriate, the individuals concerned.

As an auxiliary guide in resolving security incidents, Happenee uses the WP29 Working Group Report on Cases of Personal Data Security Violations under Regulation 2016/679 ("the Opinion").

Based on this Opinion, individual violations are classified into three basic categories:

- "Breach of confidentiality" - in case of unauthorized or accidental provision or disclosure of personal data.
- "Breach of availability" - in case of accidental or unauthorized loss of access or destruction of personal data.
- "Breach of integrity" - in case of unauthorized or accidental modification of personal data.

2. Access control rules

The purpose of managing access to information and resources of Happenee information systems is to ensure that only authorized persons have access to them. Rules are set for access to these resources, which determine the procedures for authorization, establishment, changes and withdrawal of access rights.

Access to the system is allowed to logged in persons with authorization according to the assigned authorization. Complexity requirements are specified for the created password - the minimum length of the password.

In accordance with the security policy in the processing of personal data, Happenee uses standard procedures on the basis of which access rights are defined for all positions, while the access rights of individual authorized persons are regularly reviewed. Access of authorized persons is controlled separately only to personal data that he or she needs to perform his activity.

Furthermore, procedures are introduced for removing or modifying the access rights of persons authorized to terminate or change their work, or similar relationship.

Access to the application for customers is always allowed on the basis of a generated name and password, which the customer can change and must meet the basic security settings - minimum length.

All personal data that the customer enters into the application are stored in a database on the server of the cloud service provider. Only an authorized person has access to this data.

a) Use of other platforms for the storage of personal data

Happenee's personal data is also stored primarily on virtual servers, primarily MS Azure, then virtual servers for the mail server, and Happenee uses Google Drive to distribute internal documents.

Only authorized persons have access to this personal data stored on other platforms through an account secured by a generated password.

All virtual server operators with which Happenee cooperates have been selected on the basis of a study and evaluation of their technical and security measures, which they represent on their websites, and on the basis of previous experience with these operators.

As part of technical and security measures, the operator of the MS Azur server declares on its website the implementation and compliance with the requirements of the internationally recognized standard ISO / IEC 27018, which contains a set of procedures for the protection of personally identifiable information in public clouds.

3. Asset management

Happenee is aware of all areas within which personal data is processed and can always identify the source from which the personal data was obtained and the specific owner of the personal data.

Happenee ensures that all personal data is kept for the time strictly necessary to fulfil the purpose for which the personal data was obtained and at the same time to comply with the obligations imposed by law regarding the period of retention of personal data in the records. Personal data of customers are anonymized after 5 years of inactivity.

Every Happenee employee is adequately trained in the overall management of Happenee's assets and is aware of the consequences of a breach of duty in this regard.

As part of information security, Happenee encrypts the personal data with which the authorized persons works. Happenee also shreds all documents containing personal data that is not required by law to retain.

4. Compliance with protection standards by persons authorized to process

Each person entrusted with the processing shall ensure compliance with the high standards of personal data protection with which he has been informed and shall make every effort to prevent the unauthorized processing of personal data.

A contractual relationship has been established between each processing agent and Happenee on the basis of an employment contract, a contract for the provision of services, an agreement concluded outside the employment relationship or other similar contracts or agreements.

In order to comply with a high standard of personal data protection, individual contracts and agreements contain safeguard clauses, including partial obligations, i.e., for example, a material liability clause.

Each person authorized to process is fully aware of the meaning and importance of the concept of personal data security and is aware of possible contractual arrangements in the event of a breach of this obligation.