Terms & Conditions of Security, Discreetness and Notification of Security Incidents

Article I
Representations

1. The provider undertakes to provide the agreed services or to supply the agreed goods to the receiving party.
2. The provided services do not include any processing operations carried out by the provider in respect of the personal data being processed by the receiving party. Even though the provider may, in the course of the activities carried out for the receiving party, come into contact with personal data and information about the parameters of the processing of personal data, including information on data security, the provider is not entitled to handle or manipulate with the data in any manner.
3. These Terms & Conditions constitute an inseparable part of the contract pursuant to Paragraph 1. In the event of any discrepancies between the contract and these Terms & Conditions, the provisions of the contract shall prevail.

Article II
Definitions

1. Unless expressly provided otherwise, the terms defined in Article 4 of the GDPR shall have the meaning ascribed to them in the provisions of the GDPR referred to above.
2. For the purposes of this contract, the following expressions shall have the meaning set forth below:
   a. Security incident - means a personal data breach that leads to accidental or unlawful destruction, loss, alteration or unauthorized disclosure of the transferred, stored or otherwise processed personal data, or at least the risk of accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data, or the loss or unauthorized disclosure of passwords, access data or other tools used to access the premises where the processing of personal data is carried out, the stored or processed personal data, or multimedia or computer technology used for the processing or storage of personal data; the above also applies to the information on security of the processing of personal data, accordingly;
   b. Notifier – means a person reporting a security incident;
   c. Notified person – means a person other than the Notifier who is affected by the security incident to the extent of being the originator or initiator of the security incident.

Article III
Security Measures

1. In the course of the provider's activities carried out for the receiving party, the provider is not authorized in any way to actively access the personal data being processed by the receiving party, or the information about the processing of personal data performed by the receiving party or the information about security of the processing of personal data.

2. Should the provider, in the course of the activities carried out for the receiving party, come into contact with personal data, information about security of personal data or information on the parameters of the processing of personal data, the provider shall be bound by confidentiality in respect of such information and shall ensure the provider's

employees and other persons engaged by the provider to also be bound by confidentiality to the necessary extent.

3. In the course of the activities carried out for the receiving party, the provider will proceed with maximum caution in the handling of and manipulation with the information and data carriers pursuant to Paragraph 1. The provider shall refrain from any interventions in the carriers, particularly interventions that could result in unauthorised disclosure, alteration, destruction, making unavailable, erasure or transfer of such information or data. The above shall also apply to the measures and tools implemented to secure the above data and information, accordingly.
4. The provider shall implement the necessary security and technical and organisational measures in order to fulfil the purpose of paragraphs 1 through 3 of this Article.
5. Proper security and fulfilment of the obligations pursuant to paragraphs 1 through 4 includes regular reviews of the effectiveness and adequacy of the security measures adopted, the training of employees and persons engaged in the activities for the receiving party and verification of their knowledge, correct understanding of the functioning of security rules and compliance with the applicable measures and guidelines.

Article IV
Other Measures Implemented to Ensure Security

1. The processor shall implement security measures on the basis of a proper assessment of risks, the likelihood of risks and their possible negative consequences for the rights and freedoms of the persons concerned. The primary objective must be to eliminate the risks, minimize the risks where elimination is not possible, and eliminate or at least minimize possible negative consequences for the rights and freedoms of the persons concerned where minimization of risk is not possible.
2. The Provider shall, inter alia, implement and guarantee, among other things, the following rules and principles designed to ensure security:
   a. An obligation to act in such a manner so as to prevent any loss, destruction or unauthorized alteration or disclosure of the data or information pursuant to Article III(1) and (2). In the event of imminent risk of loss, unauthorized destruction, alteration or disclosure of such data or the relevant data carriers, an obligation to take adequate steps to the necessary extent and to report to the receiving party, without undue delay, the steps taken, their reasons, progress and consequences;
   b. Every person is obliged to immediately notify the designated responsible person, by e-mail or in writing, of any defect in the conditions or individual parameters of the processing or related security;
   c. Other appropriate and necessary security measures shall be implemented, such as regular forced change of access passwords;
   d. Technical and other security features that are part of the tools and other means used in the activities performed for the receiving party shall be used to the maximum extent possible; in particular, employees shall be obliged to:
      i. lock rooms, cabinets and other areas where personal data carriers are stored, unless a person authorized to access the personal data and their carriers is present on the site;
      ii. log out, when they finish working with a technical or multimedia device or application, from the device, environment or application;

iii. keep secret and confidential passwords and login codes for access to devices, multimedia environment or individual applications;
iv. choose safe passwords, i.e. passwords consisting of at least 8 alphanumeric and non-alphanumeric characters and containing both upper and lower case;
v. if using mobile phones and other similar devices, to always use security options to start and log in to the device, as well as to unlock it, at least by entering a four-digit PIN; a higher-level of security is preferable, if possible;
vi. refrain from installing any software or making any changes to multimedia devices and computer equipment entrusted to employees for the purposes of performance of their work tasks, without the consent and assistance of the responsible person; in particular, employees are not allowed to inactivate antivirus and other similar programs designed to ensure the security of the processed personal data;
vii. if an employee is entrusted with a mobile phone or PC, or other similar multimedia device or computer technology and, particularly, if the employee is able to use such equipment outside the employer's premises, the employee is obliged to implement and consistently apply such measures as to completely exclude access to and use of such equipment by any third party, as well as measures to prevent the destruction or damage of such equipment.

Article V.
Communication

1. Any communication (by phone, e-mail, ordinary mail) relating to the activities carried out by the provider for the receiving party, whether within one Party or between the Parties or towards third parties (contractors, clients, public authorities, etc.), shall always be carried out in the most secure and discreet manner, so that no person other than the legitimate addressee can acquire knowledge of the content of the communication, including the transmitted information and data.
2. Messages containing information pursuant to Article III(1) and (2) shall be transferred using a data box, e-mail message, electronic storage service or a postal services provider or another similar method of physical delivery of the data carrier to the addressee (messenger service, etc.).
3. If possible with regard to the nature of the addressee and the provided services, a data box will be the preferable form of communication.
4. If it is not possible to use the data box, the data may be transferred using an e-mail or a postal services provider or another similar method of physical delivery of the data carrier to the addressee (messenger service, etc.), if it is required by the nature and security of the transferred information. In such cases, it is always necessary to identify the particular addressee and to use the receipt confirmation service, or the personal delivery option.
5. The transfer of information via an e-mail message pursuant to paragraph 4 is subject to proper security of the transferred information. Security means that the file being transferred will be at least compressed to the ZIP or similar file format, and encoded using a safe password. A safe password means a password with at least 8 characters containing both alphanumeric (uppercase and lowercase letters and numbers) and non-alphanumeric characters. The password must be agreed with the addressee in advance

and transferred safely; the transfer of a password in an open email message is not considered safe; the same applies to password changes.

6. The responsible representatives of the Parties shall inform each other of the agreed password in a discrete manner.

Article VI.
Security Incident

1. If the provider becomes aware of a security incident, the provider shall immediately notify the incident to the receiving party. The same applies if there are reasonable grounds to suspect a security incident.
2. The notification pursuant to this Article shall always be based on the following:
   a) honesty and integrity on the part of the notifier;
   b) the notifier's firm belief that the notification is true;
   c) the notifier's firm belief that the conduct/notification is lawful;
   d) verification of the reported information.

   Other notifications that do not meet the above criteria (unverified or dishonest notifications made with the intention to harm someone) may give rise to an obligation to compensate the harm (tangible or intangible).
3. A security incident shall be notified in a discreet manner to the person designated by the receiving party
4. The provider shall ensure that the notification by the notifier is made in such a manner that the notified person is not aware of the notification, if the notification affects the provider's co-worker or member or another person who is to be qualified as a law offender.
5. The notification shall be made in writing or by email.
6. The notification shall include the following (to the extent that it is inherently possible):
   a. the notifier's name and surname, job position and contact information;
   b. all information about the notified security incident known to the notifier and to any third parties (i.e. a description of the security incident);
   c. the names and surnames of all persons participating in the security incident, including their job positions or the institution in which they work, and identification of the notified person;
   d. the names and surnames of the persons who have any information about the security incident, including their contact information;
   e. information about how or from whom the notifier found out about the security incident;
   f. information about how the truthfulness and accuracy of the revealed information was verified by the notifier and by the processor;
   g. the processing of personal data, processing operations and personal data affected by the security incident, including the scope of affected data subject;
   h. possible risks to the rights and freedoms of data subjects, to the controller, to the processor or to third parties arising from the security incident.

   All evidence available to the provider shall be attached to the notification.
7. The notification shall be made in the Czech language.