Personal Data Processing and Security Terms & Condition – Data Processing Contract

Article I
Initial provisions

1. The Parties entered into a service contract. These Terms & Conditions constitute an inseparable part of the service contract pursuant to the preceding sentence. In the event of any discrepancies between the contract and these Terms & Conditions, the provisions of the contract shall prevail.
2. By signing these Terms & Conditions, the Parties fulfil their duties pursuant to the provision of Article 28 of the General Data Protection Regulation.
3. These Terms & Conditions regulate the rights and obligations of the Parties relating to the processing of personal data carried out by the Parties acting as the personal data controller and the personal data processor in order to ensure maximum security of the personal data being processed and of the information on data security, as well as transparency of the processing and compliance with the obligations laid down in the personal data protection legislation.
4. The positions of the Parties as either the personal data controller or the personal data processor, as well as the processing tasks of the processor, are stipulated in the contract referred to in paragraph 1 hereof.

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. The following expressions shall have the meaning set forth below:
   a. Sensitive data – means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purposes of unique identification of a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
   b. Public body – means an entity established by law and carrying out tasks stipulated by law in the public interest;
   c. Chain of processors – means a situation in which another person is engaged in the processing of personal data as a sub-processor on the basis of an agreement with the processor;
   d. Personal data sub-processor - means a person authorized by the processor to perform certain tasks in the processing of personal data carried out by the personal data processor for the personal data controller; the sub-processor and the personal data processor will enter into a contract for the sub-processing of personal data in a form corresponding to these Terms & Conditions, particularly in terms of security of the processing of personal data and security of the relevant information on the security of processing, and the fulfilment of the obligations laid down in the GDPR and in the legislation governing the protection of personal data in general;
   e. 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 and the information on processing parameters, accordingly;

f. Third country – means any country outside the European Union;
g. Transfer of personal data to a third country – means the transfer of personal data to a third country to carry out a processing operation, including the use of cloud computing, if the services are, even in part, carried out in a third country;
h. Notifier – means a person reporting a security incident;
i. 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
Key Parameters and Terms & Conditions of Personal Data Processing
Rights and Obligations of the Parties

1. In connection with the processing of personal data, the processor will ensure for the controller the following tasks and the Parties will have the following rights and obligations:
   a. Providing each other with the necessary assistance and cooperation to ensure due fulfilment of the obligations laid down in the personal data protection legislation and adequate security of the personal data being processed and the information on their security, and to respect the rights and freedoms of the data subject and to facilitate, as much as possible, the exercise of rights by data subjects;
   b. The processor will only process the personal data on documented instructions from the controller.
   c. If, in connection with the processing of personal data, the personal data are to be transferred to third countries by the personal data processor, the processor shall notify the controller of such intention in writing or by e-mail well in advance before its implementation with a request for the controller's opinion. If the controller does not provide its opinion within three business days from the receipt of the above notification, the controller shall be deemed to have approved the transfer of personal data to a third country. If the country is not a EU country, an EEC country, a country designated as a safe country by the EU Commission's decision, a country that has ratified the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, or another country where the transfer of data outside the EU would be considered safe under the EU Commission's decision, the processor has to ensure an adequate level of protection (e.g. standard contractual clauses pursuant to the Commission's decision);
   d. The personal data processor shall implement the necessary technical and organizational measures to ensure an appropriate level of security of the processed personal data and of the information on their security, as well as all other necessary

measures laid down in Article 32 of the GDPR in order to ensure security of the personal data and of the information on security of the processing;

e. The personal data processor shall only engage in the processing of the personal data a sub-processor, if the conditions stipulated herein are met;
f. The personal data processor shall provide the personal data controller with the necessary assistance and cooperation in fulfilling the controller's obligations pursuant to Articles 32 through 36 of the GDPR;
g. The personal data processor shall, on the instruction of the personal data controller, destroy, correct, modify or update the personal data being processed or the information about the processing of personal data;
h. Should a data subject exercise with the data processor any of the data subject's rights, in respect of which the data controller's obligations to the data subject are not performed by the processor on behalf of the controller, the processor shall immediately notify the data controller of this fact and provide the data controller with all the necessary assistance and cooperation in order to allow the personal data controller to duly, and within the statutory deadline, respond to the exercise of the right by the data subject;
i. The processor will maintain records of the processing operations carried out and of the related facts so that the data controller is able to demonstrate compliance with the statutory obligations, as laid down in Article 5(2) of the GDPR, in line with the principle of 'accountability'.
j. The processor will always process the personal data in such a manner that the basic personal data processing principles and obligations arising from Article 5(1) of the GDPR and from other articles implementing and complementing the provision referred to above are fully complied with. For the above purpose, the processor shall, in particular, implement appropriate internal processes and measures to ensure adequate security of the personal data being processed and of the information on their security, and ensure that persons authorized to process the personal data and persons who come into contact with the information on the parameters of personal data processing or the information on the security of personal data processing are bound by confidentiality in respect of these facts and information;
k. Upon the termination of the activities carried out for the controller, the processor shall hand over to the personal data controller or to another designated data processor, in a secure manner, all the personal data being processed and all related documents and information so as to allow for a smooth and uninterrupted continuation of the processing of personal data; in particular, if the processing of personal data is carried out by means of modern technologies, the data and related information will be transferred in an open format so that they can be used and further processed without any necessary intervention. The processor shall provide the controller with all documentation and information necessary to demonstrate the lawfulness of the processing and fulfilment of the related obligations, so that the controller is subsequently able to retrospectively demonstrate the lawfulness of the processing and compliance with the relevant obligations for a period equal to the longest statutory period of limitation or period of prescription determined for a tort or public offense, which could have been committed by the processor in the processing of personal data and for which the controller could (even to some extent) be held accountable;

l. If the personal data processor reveals or suspects any irregularities in the conditions of the processing of personal data that are the responsibility of the personal data controller or in the processing of personal data as such, the personal data processor shall notify the personal data controller of the same.

Article IV

Measures Implemented to Secure the Personal Data Being Processed

1. The level of security measures implemented to secure the personal data being processed and their carriers or the multimedia environment in which the personal data are stored or processed shall be adequate to the nature of the personal data being processed and the level of possible interference with the rights of the data subject to which they relate.
2. Security measures are measures that serve to ensure confidentiality, i.e. to prevent the disclosure of or access to the personal data and their carriers to/by any persons outside the group of persons authorized to carry out processing operations with or otherwise handle the personal data. Security measures further include measures that serve to prevent unauthorized access to and processing of the personal data as well as their unauthorized alteration, destruction, loss or deletion (e.g. making copies or backups).
3. The principle of necessity and minimization shall be observed in appointing authorized persons and assigning competencies relating to the personal data being processed; the authorization and its degree shall depend on the person's job position and the competencies assigned to such position, so that the person concerned is only able to handle such personal data as are necessary for the proper performance of his/her position. The same shall apply to determining the scope of the processing operations the person will be authorized to perform and the cases in which he/she may use its authorization. The ultimate purpose of the processing of personal data shall always be taken into account.
4. Proper security includes regular reviews of the effectiveness and adequacy of the security measures adopted, training of staff and persons who have been engaged in the processing of personal data or who are in contact with the processing information and information on the security of processing, and verification of their knowledge, correct understanding of the functioning of security rules and compliance with the measures and practices.
5. The Personal data controller is entitled to conduct, on a regular basis, either directly or through a third party, audits and inspections of compliance with the personal data processor's obligations, including a verification of sufficiency of the measures implemented to ensure security and compliance with the measures and procedures by the processor's employees.
6. If, on the basis of a review/audit/inspection or other findings, the data controller brings to the attention of the data processor any irregularities regarding the performance of the processor's obligations, the processor shall remedy the situation without undue delay. The processor will notify the controller of the remedy.
7. The provisions of this article shall also apply to ensuring security of the information on security of the personal data processing, accordingly

Article V

Other Measures Implemented to Secure the Personal Data Being Processed

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 data subjects. 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 data subjects where minimization of risk is not possible.
2. The processor shall, inter alia, implement and guarantee, among other things, the following rules and principles designed to ensure security of the processed personal data and the security of their carriers and multimedia devices:
    a. An obligation to act in such a manner so as to prevent any loss, destruction or unauthorized alteration or disclosure of the processed personal data or information about their security. In the event of imminent risk of loss, unauthorized destruction, alteration or disclosure of personal data or information about their security, an obligation to take adequate steps to the necessary extent and to report to the responsible person, without undue delay, the steps taken, their reasons, progress and consequences;
    b. No one is allowed to handle the personal data and carry out processing operations beyond the scope of his/her authorization, outside the purpose of processing or without the legal ground for the processing operations and the fulfilment of all other legal obligations arising from the legislation governing the protection of personal data;
    c. Every person is obliged to immediately notify the responsible person, by e-mail or in writing, of any defect in the conditions or individual parameters of the processing of personal data;
    d. When the processing of personal data is carried out using, in particular, modern technologies, backups of the processed personal data and of the related data and information about the processing shall be made at such intervals so as to ensure continuity of processing, and keeping the processed personal data up to date and accurate even in the event of change or destruction of the personal data being processed; if the processed personal data are to be restored from the backup, the responsible person shall ensure, based on the information on and records of the processing of personal data, that the processing of personal data is brought into line with the data subjects' rights previously exercised, as well as with other statutory obligations;
    e. Other appropriate and necessary security measures shall be implemented, such as regular forced change of access passwords;
    f. Technical and other security features that are part of the tools and other means used to process the personal data 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 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.

The provisions of this paragraph also apply to the security of information on security of the processing of personal data, accordingly.

Article VI
Communication

1. Any communication (by phone, e-mail, ordinary mail) relating to the processing of personal data, 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 personal data.
2. Personal data shall be transferred using a data box, an e-mail message, an 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, the data box will be the exclusive form of communication. In these cases, it is not possible to transfer personal data by phone, e-mail or otherwise.
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.). 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 personal data via an e-mail message is subject to proper security of the transferred personal data. 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 select a secure password and shall inform each other of the password in a discrete manner.

7. The transfer of personal data by phone may only be used in exceptional cases; the use of phone includes short text messages (SMS), multimedia messages (MMS) or mobile applications with similar functions. Personal data can only be provided by phone if: the identity of the caller has been securely verified, it is certain that no person other than the duly identified caller can attend the call, and if the data are transferred between the controller and the processor, between two controllers, or between the processor and a sub-processor, it is certain that the data are properly recorded. If data are transferred using an SMS, MMS, or an application with similar functions, the message shall be deleted immediately after the data have been properly recorded.

Article VII
Security Incident

1. If the personal data processor becomes aware of a security incident, the processor shall immediately notify the incident to the personal data controller. 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) suffered by the controller, the notified person or other affected persons (family members of the notified person, etc.).
3. A security incident shall be notified in a discreet manner to the person designated by the controller
4. The personal data processor 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 processor'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 processor shall be attached to the notification; Article VII shall apply accordingly.

7. The notification shall be made in the Czech language.

Article VIII
Terms & Conditions of Engaging a Sub-processor

1. The personal data processor is entitled to engage a sub-processor in the processing of personal data.
2. The personal data sub-processor may be a person who will sufficiently guarantee the implementation of adequate technical and organizational measures to ensure compliance of the processing with the personal data protection legislation and safety and protection of the personal data and the rights and freedoms of the data subjects. The personal data processor shall be liable for a proper verification of reliability of the sub-processor the processor intends to engage in the processing of personal data.
3. The personal data processor shall notify the personal data controller in writing of an intention to engage a sub-processor in the processing of personal data. The personal data controller shall have the right to object to the engagement of a personal data sub-processor; alternatively, the controller reserves the right to approve the person who will act as the sub-processor. If the controller fails to inform the processor of its decision concerning the approval of engagement of a sub-processor within 5 business days from the date of receipt of the notification of an intention to engage a sub-processor in the processing of personal data, the processor of personal data shall be allowed to engage a sub-processor in the processing of personal data.
4. The personal data processor shall oblige the sub-processor to fulfil the obligations stipulated in the personal data protection legislation and to ensure security of the personal data being processed and the information on their security at least to the extent laid down herein. The same applies to other content of these Terms & Conditions.
5. The personal data processor is liable to the personal data controller for the activities carried out by the personal data sub-processor as if the activities for the controller were carried out or the obligations fulfilled by the processor.

Article IX
Joint Provisions

1. Upon the personal data controller's request, the processor will, without undue delay, make available to the personal data controller or to a person designated by the controller the personal data being processed or a particular part thereof, as well as the information concerning the processing of personal data, including the information on security of the processed personal data.

2. Upon the personal data controller's request, the processor will, without undue delay, provide to the personal data controller or to a person designated by the controller a copy of the personal data being processed in the manner and format allowing for further processing of the provided personal data. The same applies to the information on the processing of personal data and their security.

3. Upon the personal data controller's request, the processor will, without undue delay, submit to the personal data controller the documentation as evidence of the fact that the processing of the personal data carried out by the processor in favour of the controller has the relevant and valid legal ground.