TABLE OF CONTENTS

1 STANDARD CONTRACTUAL PROVISIONS IN THE SPHERE OF PROTECTION OF INFORMATION SYSTEMS

1.1 DUTIES WITHIN THE FRAMEWORK OF GENERAL SECURITY

The duties of the Service Provider (contractor, etc.) is to introduce necessary technical and organisational measures providing for security of the services, including the Client's information system and data, with the aim of:

- keeping an adequate standard of the eligible security of information systems for the services rendered in accordance with the contractual conditions and terms (qualification, authorisation, and certification conditions) and be capable of proving the compliance with them upon request. At the same, the Service Provider must also demonstrate its sufficient knowledge about the required technologies and its own necessary expertise,
- providing for confidentiality, accessibility, and integrity of the Client's information system, all this up to the extent of the ordered services to it,
- protecting all information, data, and figures against their disclosure, modification, destruction, loss, distortion, unauthorised access & processing, and all this against activities either accidental or unauthorised or illegal, and
- providing for monitoring and auditing of operations run in the course of information & data processing as well as technical measures leading to mitigation of risks and consequent security accidents.

The Service Provider undertakes to demonstrate, upon a request from the Client's side and without undue delay that such measures are in place for the whole duration period of the contract.

The security policy, procedures and measures implemented by the Service Provider or, as the case may be, upon the Client's instructions, must be in any case duly documented, made accessible to the Client and modified by reflecting the sensitivity of the rendered services, and they must be for the whole time in accordance with the legislation and practice applicable in the relevant sphere.

1.2 DUTIES RELATED TO THE PROTECTION OF THE INFORMATION SYSTEM OF THE SERVICE PROVIDER

With regard to the Client's data sensitivity that might be processed in the information system of the Service Provider, the Service Provider will pay a special attention for providing for physical and logical security of the information system used for the Client's data processing.

If the information system of the Service Provider processes the Client's data, then Service Provider must provide for the following:

- Protection, confidentiality, accessibility and integrity of its information system; security measures implemented by the Service Provider must be documented and in line with the legislation and industrial practice applicable to the relevant sphere and at an adequate level.
- Backing up of the data necessary for the service itself and the Client's data, as needed and upon the Client's request so that both services and data will be possible to renew according to the contractual conditions.

- The backup and renewal procedures will be set and handed over to the Client at the beginning of rendering the service. In particular, it will include responsibility, periodicity, technical parameters, access control procedures, and data renewal procedures, including review processes. The Service Provider undertakes to test regularly, at least once a month, and the data renewal procedure and, upon request, to inform the Client about the test results.
- Keeping and processing of the Client's data that must be stored separately from the data of the Service Provider and/or the data belonging to third parties.
- Implementing of the authorisation control systems of for all users (personal accounts, technical accounts, etc.) who have the access to the Client's data through controlled logical and physical accesses.
- Upon the Client's request, submitting without undue delay all tracks and records (e.g. audit logs, extraordinary events and security accidents) and all security analyses carried out by the Service Provider for the whole duration period of the contract.
- Implementing of the security policy focused for keeping the records usable for a period of one year, and in addition records of activities and/or attempts of activities carried out on the information system of the Service Provider (e.g. incoming/outgoing data flows, new versions of software applications, test results, calculations of errors, removals of duplicities, data erasures, etc.) for the purposes of audits (checks) or for means of evidence. The records must contain the service source and objective, type of an event, user/system identification, and exact time information.
- Implementing of relevant measures within forty-eight (48) hours from the identification of a problem or a threat that may influence the information system of the Service Provider, and adequate strengthening of security measures or any other solutions allowing reacting effectively to such incident/threat. The Service Provider undertakes to inform the Client about such incidents/threats without undue delay.

The Service Provider undertakes to prove that the above-specified measures were continuously implemented through the whole duration period of the contract, and this without undue delay after the Client's request.

The Service Provider undertakes to inform the Client about the localities (country, city, street) where the Client's data and information are processed and kept and on what hosting they are present. The above-mentioned geographical regions are defined in the contract.

The Service Provider and/or the subcontractor approved by the Client in writing will be entitled to use such a locality only if it is agreed in the contract or subsequently approved by the Client within a framework of a rider to the contract.

1.3 SECURITY OF PRODUCTS AND SERVICES SUPPLIED BY THE SERVICE PROVIDER

Vulnerability *means any defect, weakness, or error in the design or malware influencing the relevant products and/or services covered by the contract.*

Serious vulnerability *means such vulnerability, which may lead to serious impacts to the information and data, and/or to the Client's information system.*

The Service Provider undertakes to:

- if a new case of a serious vulnerability is identified, submit to the Client within eight (8) working days from the vulnerability identification moment, an analysis of impacts and plan of remedial measures in accordance with the Client's requirements
  - to submit to the Client within two (2) working days from the vulnerability identification moment, any mitigating or temporary solution, which however, must not in any way change the price and/or functionality of the products and the services supplied under the contract,
  - to submit to the Client a final solution of the problem within five (5) working days from the vulnerability identification moment,
- if a new case of a vulnerability is identified, where the vulnerability is NOT classified as a serious vulnerability:
  - to submit to the Client within four (4) working days from the vulnerability identification moment, any mitigating or temporary solution, which however, must not in any way change the price and/or functionality of the products and the services supplied under the contract,
  - there, where no suitable remedial measure is in place within four (4) working days from the vulnerability identification moment, the Client will be submitted with a final solution for the problem removal within eight (8) working days from the vulnerability identification moment, and the Client will be regularly informed about the steps taken by the Service Provider,

- to supply to the Client, from the side of the producer/developer a software application necessary for the vulnerability removal,

- to inform the Client, broadly speaking, about the risks connected with the security and protection of information systems and offer implementations of concrete measures for the detection of attempts on infringement and security incidents together with the relevant costs subject to the Client's approval.

1.4 OBLIGATIONS IN CASES, WHERE THE SERVICE PROVIDER USES THE CLIENT'S INFORMATION SYSTEM

The Service Provider undertakes to use only such sources and means for the connection to the Client's information system that are provided by the Client, and this solely for the purposes of rendering the services agreed within the scope of the contract and in a strict compliance with the security policy of the Client's information system that are handed over to the Service Provider. In this regard, the Service Provider is NOT entitled, without an express authorisation from the Client's side, to use, disseminate, or transfer confidential information and data of the Client outside the Client's information system.

There, where the employees of the Service Provider may have an access to the Client's information system, and where they are expressly authorised in advance to such access, either within the work tasks in the Client's premises or in form of a remote access, the security policy of the Client's information system requires that such employees are continuously acquainted with the documents related to the security of information systems that are intended for them and that they follow them.

The Service Provider will ensure that its employees are informed and trained on a regular basis with the documents intended for them, and this even before their allotments to the relevant tasks or during the first several days, during which they are provided with them by the Client.

1.5 INFORMATION AND REPORTING DUTIES

The Service Provider will be obliged:

- to inform the Client without undue delay about any security incident that takes place in its information system (including a third party unauthorised access, data losses, data integrity impairment, importation of malware and/or non-standard use of information systems used for the services rendered to the Client), and this at any time, where such incident may influence the information system, services, information and data of the Client with regard to the rendered services,

- to provide for the compliance with these duties by the employees charged with such tasks and ensure that they are regularly informed about them,

- to inform the Client about any organisational changes and technical modifications that might have negative effects to the security of the Client's data and information.

- to implement regular monitoring stipulated by the Client with the aim of reducing risk of theft of the Client's information and data or unauthorised access to them by any third party or any other user acting on behalf of the Client,

- to implement methodology of controlling of security incidents, which describes detection process of security incidents, responses and tripping of contingency management processes; this methodology and its potential changes will be subject to a prior written approval of the Client,

- to render assistance to the Client, and this without any claim for an additional fee, in the course of adopting of remedial measures or coping with security incidents, including reporting to the relevant authorities and persons that might be damaged by such infringements,

- to specify, without undue delay, backup and remedial procedures for coping with all these incidents, including their impacts on the protection of the Client's information system and security of its information and data.

The Service Provider is obliged to submit to the Client, upon its request, the results of security audits of the Service Provider's information system (in particular: identified risks and vulnerabilities) in the relation to the services rendered, where the audits are performed at least once a year by a third party for any product and software licenced by the Service Provider at the transition to the operational mode or at any significant change and/or update. The Service Provider undertakes to implement security measures for the whole life cycle, starting with the development, through the realisation and ending with live operations, where it will be necessary to demonstrate to the Client settings of processes and technologies that are aimed to reduce risks and improve quality of codes, products, or services of the Service Provider.

1.6 MALWARE

*The term **"Malware"** means a malicious computer code, including specific viruses, logic bombs, Trojan Horses, worms, or any other codes or instructions infecting or attacking any programs, software applications, data, files, databases, computers, or any other hardware and its components, where they damage or* disclose confidential data *or endanger their integrity and, in doing so, they disturb some or all operations, occupy some or all part of information systems and enable the system operations deviate from their purported objectives.*

The Service Provider will adopt all necessary preventive measures against importation of malware into the information system that may contain the Client's data and information and, in addition, also such adequate measures that can detect the existence of malware. To this purpose, the Service Provider will conduct adequate security tests and it undertakes to check the information system components before they are supplied to the Client.

For the cases when malware is already imported into the information system, the Service Provider and the Client have agreed that they will proceed in mutual harmony in order to find the source and repair the damage without undue delay.

If it is found that such infection or malware importation can be attributed to the Client, then the Client will bear the costs of diagnostic procedures and renewal of the relevant systems or services.

If it is found that such infection or malware importation can be attributed to the Service Provider, then the Service Provider will bear the costs of diagnostic procedures and renewal of the relevant systems or services.

If the contact persons of both parties do not agree on the identification of such culpability, then they will proceed according to the steps stipulated for dispute resolution in the contract.

1.7 DUTIES OF THE SECURITY DEPARTMENT OF THE SERVICE PROVIDER

The Service Provider is obliged to appoint a security & risk control manager who will be the only contact place for the Client as regards these issues. (It is also possible to contact the Data Protection Officer (DPO) according to the REGULATION (EU) 2016/679).

1.8 CHECKS AND AUDITS

The Service Provider undertakes to ensure that the risk control level is continuously monitored and that the security policy and rules applied to the services are observed, which includes its subcontractors as well.

1.8.1 Technical security audits

The Service Provider agrees that the Client is entitled to conduct technical audits (including scanning, automatic testing of vulnerabilities, infiltration tests, configuration, and infrastructure audits) in the information system of the Service Provider and in information systems of third parties – subcontractors, incl. those companies that hosts, either partially or fully, the information system of the Service Provider. The Client is entitled to assign the audit performance to a third party, with which a non-disclosure agreement will be signed, where the Service Provider will be also a contracting party to this agreement. The Czech National Bank will be entitled to carry out the audit even without such agreement.

The technical audit performance will be enabled to the auditor. These tests will consist of sets of performed tests, either automated or manually performed, from outside or inside the information system of the Service Provider, or in the information system of any of the subcontractors involved in rendering of the relevant services, with the objective to identify any vulnerabilities that may enable to the users to infiltrate to the tested system.

In this respect, the Service Provider guarantees that it is the holder of necessary and sufficient rights and authorisations for carrying out of the above-mentioned technical audits in the relevant information system and the information systems of all third parties that might be involved or otherwise concerned.

These technical audits will be subject to an advance notice given to the Service Provider and not disturbing rendering of the services.

By this, it is mentioned that it is not the purpose of these audits to enable to the Client any access to the data of other clients of the Service Provider, but only to verify the system and infrastructure security, within which the services are rendered.

1.8.2 Settlement of shortcomings

The vulnerabilities identified in the audit will be evaluated and they will be handled according to the conditions set out in the "Security" section, in the article "Security of products and services supplied by the Service Provider".

If the Service Provider fails to provide for the remedy of the shortcomings identified in the audit within the required deadline, then the Client will be automatically entitled to withdraw from the contract without any prior notice given and this withdrawal will not affect in any way the Client's claim for any damages that might be exacted under such circumstances.

1.9 OTHER COVENANTS IN THE SPHERE OF PROTECTION OF INFORMATION AND DATA

The Service Provider will train its employees in the sphere of protection of information and data (information, data, personal data, etc.) particularly with regard to current and effective legal and regulatory requirements (such as Act No. 21/1992 Coll. of 20 December 1991, on Banks, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR - General Data Protection Regulation).

The Service Provider is obliged to monitor updates and amendments of the above-specified legislative rules and, where appropriate, to react to them.

In regular intervals, the Service Provider will be proving to the Client, at least once in two years, correct performance of the data protection, including the training courses, and all this in the form of an external audit.

The Service Provider will ensure that the processed data do not leave the Client's security perimeter.

a. The security parameter for the data processed outside the information system (e.g. printed documents) is defined by an enumeration of buildings / rooms that are under a continuous security protection of the Client / Service Provider, where the data are processed, in particular: see the place of performance under the contract.

b. The security parameter for the data processed within the information system is defined by the equipment under the management of the Client, and exceptions may be granted only upon a formal application and a written approval of the Client, where the following minimal conditions must be met.

   i. The data will be processed only in the HW equipment fully under the management of the Service Provider (no processing within the cloud computing is permissible).

   ii. The data will be safeguarded against potential thefts of portable HW components by encrypting.

   iii. General security standards are applied to the hardware of the Service Provider used for data processing that is based on a consistent application of access rights; security records are made about important events.

   iv. Any room with other HW equipment is locked and the access to it is strictly limited only to selected employees of the Service Provider; the room forms a regime workplace.

   v. The data are backed up in standard procedures of the Service Provider.

   vi. Electronic transfers of the data handed over by the Client are not possible outside the network intended for the data transmissions agreed by and between the contracting parties.

Cloud computing – is a model applied in the sphere of information and communication systems and technologies that makes it possible to acquire the network access to configurable computing means (e.g. networks, servers, data warehouses, applications, and services) that are shared by a larger number of users and the capacity of which is provided and again released a with minimum demand for its administration or intervention from the side of the cloud computing provider.

Application of the European regulations on data transfers outside the EU

The Service Provider will ensure that no data from the Client, i.e. including personal data of natural persons will be transferred outside the member states of the European Union by the Service Provider and/or any other person acting in the name of the Service Provider and/or any subcontractor. The Client will be entitled to check if this condition is met.

If agreed so with the Client, the Service Provider will be entitled, in the scope necessary for the performance under the contract, to use data processing sources in the state that does not provide for an adequate level of the data protection according to REGULATION (EU) 2016/679 (GDPR) provided that all standard contractual clauses are concluded as they are stipulated in Article 46 of the GDPR. Upon the Client's request, these clauses will be signed by the Service Provider, subcontractor, and if involved in the processing, by the Client. The Service Provider will provide for signing and compliance with these clauses from the side of the Service Provider. If it is required that such transfer is subject to the approval of the Office of Personal Date Protection or similar regulatory authority, it will be possible to get the relevant data processed in a third country only if such approval is obtained aside from the above-specified clauses, if they are necessary according to the GDPR (for more details see Article 46 of the GDPR).