Data Processing Terms requestor.com s.r.o.

concluded in accordance with Article 28(3) of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as "**GDPR**").

These Data Processing Terms regulate the rights and obligations in the processing of personal data by **requestor.com s.r.o.**, incorporated under the laws of the Czech Republic, business ID No. 28349121, registered office at Purkyňova 649/127, Medlánky, 612 00 Brno, the Czech Republic, registered in the Commercial Register under file No. C 62914 at the Regional Court in Brno (hereinafter referred to as "**Requestor**" or the "**Processor**").

These Data Processing Terms (the Terms) form an integral part of the Agreement concluded between you and Requestor if you are the controller or processor of the personal data (hereinafter referred to as the "**Controller**"), and Requestor is in the position of a processor or further processor of such personal data based on this Agreement.

1. Interpretation of Terms

1.1. In these Terms, Personal Data means personal data (within the meaning of Article 4 of the GDPR) processed by the Processor on behalf of the Controller, which occurs in the course of performance under the Agreement.

1.2. Agreement means the Requestor Service Agreement, the Requestor Software as a Service Solution Distribution Agreement or the Requestor On-Premises Solution License and Service Agreement concluded between the Processor and the Administrator.

1.3. The terms data subjects, personal data breach, data processing and supervisory authority have the meaning stipulated in the GDPR.

2. Roles and Data Procession Instructions

2.1. The Processor undertakes to process personal data for the Controller exclusively based on documented instructions from the Controller, unless such processing is already required by European Union or Member State law applicable to the Processor.

2.2. In particular, a contract concluded in writing between the parties based on which the processing of personal data is carried out shall be deemed to be documented instructions from the Controller.

2.3. If the Controller is in fact the processor of all or some of the personal data within the meaning of the GDPR, it warrants to the Processor in such a case that its instructions and actions in relation to the personal data, including the designation of the processor as an additional processor of such personal data, have been agreed in writing by the relevant controller.

2.4. By entering into the Agreement, the Controller declares and confirms that it has thoroughly read, understands and agrees to these Data Processing Terms.

3. Duration of the Processing

3.1. Data processing hereunder shall be carried out until the deletion of all personal data in accordance with this Article.

3.2. Upon expiration or termination of the Agreement, regardless of the manner or reason, the Processor shall within 1 month delete all the personal data and its existing copies unless Union or Member State law requires storage of the personal data.

4. Nature and Purpose of the Processing

4.1. The Processor shall process Personal Data in ways consistent with the Agreement and these Data Processing Terms, solely for the purpose of performing under the Agreement, unless otherwise agreed between the parties.

5. Types of Personal Data

5.1. The Processor will process the data collected by the Controller in the course of its activities, in particular the identification and contact data of the data subjects (e.g. name, surname, e-mail address, telephone number, ID number, VAT number, IP address) and other personal data that the data subjects voluntarily provide to the Controller for processing as part of the requirements.

5.2. The personal data concern the following categories of data subjects:

a) of the Controller's employees;

b) customers or business partners of the Controller;

c) users of the Controller, if the Controller is a customer; and

d) users of the Controller's customers, if the Controller is a distributor.

5.3. The Processor shall not process any special categories of personal data as defined by Article 9 of the GDPR or personal data relating to criminal convictions and offences as defined by Article 10 of the GDPR.

5.4. The Controller shall immediately inform the Processor in writing in case that (1) the personal data specified in Clause 5.3 of these Terms or (2) different types of personal data than those defined in Clause 5.1 of these Terms should be processed by the Processor, and provide the Processor with any and all required cooperation in order to process such personal data in accordance with applicable laws and legal regulations. Any increased costs of such data processing shall be borne by the Controller.

6. Rights and Obligations of the Parties

6.1. It is exclusively the Controller's duty, and it shall be liable for:

a) informing the data subjects about personal data processing, obtaining data subjects' consents to the processing (if necessary), and for handling all data subject's requests regarding the exercise of their rights under Articles 15–21 of the GDPR,

b) carrying out all required notification duties towards the supervisory authorities and data subjects related to the personal data processing, including but not limited to notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject.

6.2. The Controller is exclusively responsible for becoming acquainted with all the relevant terms and evaluating all the Processor's undertakings and adopted technical and organizational security measures regarding the Controller's needs, especially the Controller's data protection obligations under the governing law and legal regulations.

6.3. The Controller has thoroughly inspected and evaluated the technical and organizational measures to ensure personal data security adopted and maintained by the Processor prior to executing the Agreement, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. By executing the Agreement, the Controller confirms to the Processor that the security measures adopted and maintained by the Processor hereunder ensure a level of security appropriate to the risk.

6.4. If the Processor receives any request from the data subject while processing the data, it shall inform the data subject that he or she should contact the Controller directly with his or her request. The Controller shall be responsible for dealing with such request.

6.5. Throughout the processing of personal data under the Agreement, the Processor undertakes to:

a) adopt and comply with the agreed technical and organizational measures set out in **Annex A** to these Data Processing Terms ("**Security Measures**") to ensure the level of security of personal data required by the Controller,

b) ensure that the Security Measures are adhered to by its employees, other cooperating persons or suppliers in the scope corresponding to their activities, including ensuring that the persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,

c) to the extent proportionate to the nature of the processing and the information available to it, the Processor shall assist the Controller in ensuring appropriate technical and organizational measures to safeguard personal data, in reporting personal data breaches to the supervisory authority, in notifying personal data breaches to the data subject, in assessing the impact on the protection of personal data and in prior consultation with the supervisory authority,

d) provide the Controller with the necessary information that may be reasonably requested from the Processor to comply with the Controller's obligations to respond to requests to exercise the rights of data subjects under generally binding legislation relating to the protection of personal data,

e) to make available to the Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and to enable and contribute to audits, including inspections, carried out by the Controller or any other auditor authorised

by the Controller – audits and inspections shall be carried out strictly in accordance with **Annex B** to these Data Processing Terms, and

f) maintain a record of all categories of processing activities carried out on behalf of the Controller and make these records available to the supervisory authority on its request.

6.6. The Processor is liable for the breach of these Terms by any person which it has authorized with personal data processing (for example its employees, other persons in a similar position towards the Processor or its suppliers), including all other processors engaged by the Processor.

7. Other Processors

7.1. The Processor has been authorized to engage other processors, unless the Controller objects in writing.

7.2. The Processor shall inform the Controller in writing of any intended changes relating to the recruitment or replacement of additional processors at least 1 week before the intended change. During this period, the Controller shall have the right to object to the change. If the Controller does not object, the Controller shall be deemed to agree to the change.

7.3. The Processor undertakes to keep an updated list of all other engaged processors and to provide this list to the Controller on demand.

7.4. If another processor is involved in the processing of personal data in accordance with these Terms, the Processor shall ensure that the other processor complies with generally binding legal regulations, in particular the GDPR, when processing personal data.

7.5. The Controller shall be entitled to object to the involvement of a particular further processor in the processing of personal data at any time, even after the expiry of the period referred to in paragraph 7.2 of these Terms. In such a case, the parties shall agree on how to resolve the situation (e.g. by replacing the additional processor, accepting appropriate safeguards or withdrawing the controller's objections).

8. Confidentiality of Information

8.1. The Processor is obliged to maintain the confidentiality of the personal data it processes for the Controller. Compliance with the obligation of confidentiality means not to disclose or make available personal data to a third party, except to another processor to whose involvement the Controller has not objected, and not to use the personal data for any purpose other than the agreed purpose.

9. Indemnity

9.1. If a third party, including a public authority, makes any claim against the Processor in connection with a breach of the Agreement by the Controller, the Controller undertakes to conduct out-of-court negotiations with the third party and to defend the Processor in any court, arbitration or other proceedings, all at its own expense; this shall not apply if the claim made by the third party is manifestly unfounded. If the Processor is required, because of a settlement approved by the Controller or a final decision of a court or other authority, to pay any compensation or penalty

to anyone as a result of a breach of the Terms by the Controller, the Controller agrees to pay such compensation and penalty to the Processor. Compensation or penalty in this case includes, but is not limited to, damages, lost profits, disgorgement of unjust enrichment, reasonable monetary compensation, monetary penalty, fine or penalty.

10. Final Provisions

10.1. These Data Processing Terms include the following appendixes:

a) **Annex A –** Security Measures,

b) **Annex B –** Rules for Conducting Audits and Inspections.

10.2. The Terms have been written in Czech and English. All obligations of the Parties under these Terms shall be performed in Czech or English. In case of differences between the two documents, the Czech version shall prevail.

Annex A

Security Measures

The Processor shall implement and maintain the security measures set out in this Annex when processing personal data. The Processor shall be entitled to update or modify these measures provided that the updates or modifications do not result in a reduction in the overall security of the personal data. The Processor shall inform the Controller in writing of any intended changes concerning the modification of the security measures. During this period, the Controller shall have the right to object to the change. If the Controller does not object, the Controller shall be deemed to have consented to the change. If the Controller objects, the Processor shall not implement the change until the parties have agreed in writing on its content.

All obligations contained herein apply only to the internal systems of the Processor that it uses to process personal data.

1. Risk-based principle

1.1. During the term of the Agreement, the Processor shall, at regular intervals at its discretion, review the information security risks associated with the Controller's personal data and critical assets.

2. Organizational Security

2.1. The Processor shall take such measures to safeguard personal data against human factors risks, in particular:

a) adoption and maintenance of internal security policies and documents,

b) regular training of staff on the rules for handling personal data and information security risks,

c) ensuring contractual responsibility of employees, external collaborators, contractors and other third parties with access to personal data,

d) adopting and maintaining processes around the handling of the Processor's key assets, including the Controller's personal data.

3. Technical Measures

3.1. The Processor shall take adequate technical measures to protect personal data, in particular:

a) anti-virus solutions to protect against malware;

b) network security solutions combining firewalls, network element configuration and other technologies;

c) tools for auditing the handling of sensitive data by the administrator, configured for automated reporting of incidents to those responsible;

d) encryption of the processor's hard drives and external media; and

e) Data Loss Prevention (DLP) solutions to enforce secure data handling rules and reduce the risk of data breaches.

f) backup of critical infrastructure and data.

4. Physical Security

4.1. To protect personal data in written form and to physically protect IT equipment, the Processor shall implement, in particular:

a) access control to personal data; and

b) physical security of premises and physical/digital data storage facilities.

Annex B

Rules for Conducting Audits and Inspections

1. After the Processor receives a request from the Controller for an audit or inspection, the parties shall agree in advance on: (a) the possible timing of the audit, the security measures and how to ensure compliance with confidentiality obligations during the audit; or (b) the expected start, scope and duration of the inspection, the security measures and how to ensure compliance with confidentiality obligations during the inspection.

2. If the parties do not agree on all the necessary details of the audit or inspection in accordance with point 1 of this Annex within 2 weeks of the date on which the Processor receives the Controller's request, the Processor shall itself determine the date, conduct and other details of the audit or inspection, considering the equitable interests of the Controller.

3. For the purposes of the audit or inspection, the Processor shall make available to the Controller or to an auditor authorised by the Controller its own premises, facilities, storage and systems where personal data are processed for the Controller.

4. The Processor may object in writing to any auditor who has been appointed by the Controller if, in the opinion of the Processor, the auditor is not sufficiently qualified, is not independent, is in a competitive position with the Processor, is otherwise manifestly unsuitable, or without assigning a reason. Based on these objections, the Controller shall first select another auditor. If objections are subsequently raised with that other auditor, the Controller shall consider the objections and, if it finds them to be justified, carry out the audit itself.

5. The fees of the auditor appointed by the Controller shall be paid by the Controller. However, should the audit or inspection reveal serious breaches of the conditions by the Processor, the fees of the auditor shall be paid by the Processor. If violations by both parties are detected, the Controller shall pay the entire fee of the auditor.

6. The costs and damages associated with the audit or inspection shall be borne by each party. However, if the audit or inspection (1) is conducted for the second or more frequent time in a calendar year and (2) does not reveal a material breach by the Processor, the Controller shall reimburse the Processor for the damages caused by the audit or inspection (including, but not limited to, costs associated with curtailment of operations and compensation for lost time).

7. The Processor shall use its best efforts as may be reasonably required to ensure that these rules are also applicable to audits and inspections carried out on other Processors engaged in processing by the Processor in accordance with the Agreement and these Terms. However, audits and inspections of other processors may be governed by the individual terms and conditions of those other processors (e.g. Microsoft Azure), or compliance with generally applicable law, in particular the GDPR, may be evidenced by the other processor's own audit report or by other means of the other processor.