Data Processing Agreement
- General Part -

the **Szentkirályi Magyarország Ltd.** (seat: INFO PARK „C" Building 5th Floor, 4. Gábor Dénes Str. 1117 Budapest; tax number: 13079026-2-44) – hereinafter referred to as **Data Controller** – the Data Processing Agreements concluded by the Data Controller pursuant to Article 28 of the Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union (hereinafter referred to as "GDPR") referring to this document as the General Part, contain the general contents as follows:

1. **Duration and termination**

   1.1. This Data Processing Agreement is concluded for the same duration as the Principal Agreement. The Parties, given that they are obliged to conclude a Data Processing Agreement for as long as the cooperation between them under the Principal Agreement is in force, exclude the right to terminate this Data Processing Agreement independently. This Data Processing Agreement shall terminate if the Principal Agreement is terminated for any reason.

   1.2. This Data Processing Agreement may only be validly amended and supplemented in writing. Any waiver of formality must also be in writing.

   1.3. If any provision of this Data Processing Agreement is or becomes invalid or unenforceable in whole or in part, or for legal reasons can no longer be enforced in accordance with the intentions of the Parties, the validity of the remaining provisions of this Processing Agreement shall not be affected. Accordingly, the Parties shall cooperate to develop a valid provision to replace the invalid provision, which is suitable to achieve the purpose of the invalid provision, if the Parties' intentions remain the same despite the changed circumstances.

   1.4. The Data Controller and Data Processor agree that following the termination of the data processing, the Data Processor shall return all personal data and copies thereof to the Data Controller at the time specified by the Data Controller, but no later than within 24 hours, and shall destroy, irretrievably delete all data and copies in its possession and provide the Data Controller with credible evidence that this has been done.

2. **Provisions applicable to the Data Controller**

   2.1. The Data Controller shall provide or make available to the Data Processor data necessary and sufficient for the performance of the tasks set out in the Principal Agreement, in particular, but not limited to personal data and health data which are considered as special category of personal data and the related economic, organisational and technical information.

   2.2. The Data Controller shall be responsible for ensuring that the data transmitted or made available to the Data Processor have been lawfully collected, processed and made available to the Data Processor.

2.3. The Data Controller is responsible for ensuring the data quality of the data transferred to the Data Processor.

2.4. The Data Controller shall provide the Data Processor with instructions on data management. Instructions may be contained in the Principal Agreement or in written instructions from the Data Controller.

2.5. The Data Controller is responsible for the lawfulness of the instructions given by the Data Controller. The Data Processor shall bring to the attention of the Data Controller without undue delay, before the instruction is carried out, if it becomes aware that the Data Controller is giving inappropriate or unprofessional instructions, or if it considers that the instruction is in breach of the GDPR or the data protection provisions applicable to the Data Processor. The Data Processor shall be liable for any infringements resulting from a procedure other than those instructed by the Data Controller or without the Data Controller's instructions, unless the Data Processor has drawn the Data Controller's attention to them.

2.6. The Data Controller shall notify the Data Processor without undue delay, but no later than within 3 (three) working days, if the legal basis for the processing of personal data ceases to exist.

3. Provisions applicable to the Data Processor

3.1. The Data Processor may not take any substantive decision regarding the processing. The Data Processor may act only on instructions from the Data Controller, may use the data received from the Data Controller only for the purposes set out in this Annex and may only carry out operations on the data as set out in this Annex. Data Processor may not disclose them to third parties without the prior written consent of the Data Controller, including the authorisation of further processing by third parties.

3.2. Data Processor in accordance with applicable law:

3.2.1. processes personal data solely on the basis of written instructions from the Data Controller, including the transfer of personal data to a third country or an international organisation, unless the processing is required by EU or Member State law applicable to the processor, in which case the Data Processor shall notify the Data Controller of that legal requirement prior to processing, unless the notification of the Data Controller is prohibited by the relevant legislation on grounds of important public interest,

3.2.2. ensures that the persons authorised to process personal data are bound by an obligation of confidentiality or are subject to an appropriate obligation of confidentiality based on law. The Data Processor shall take technical and organisational measures concerning data security as instructed by the Data Controller, in this context, the Processor shall in particular ensure that access to the stored data is only possible via an internal system or by direct access by authorised persons and only in connection with the purpose of the processing. The Processor shall ensure the necessary regular maintenance and development of the tools used. The Processor shall ensure adequate physical protection of the storage device(s).

3.2.3. requires confidentiality during the processing of personal data by the Data Processor and persons acting under its authority who have access to the personal data in the

context of the processing of personal data within the framework of the Principal Agreement,

3.2.4. in the performance of its duties, assists the Data Controller in fulfilling its obligation to respond to requests related to the exercise of the rights of the data subject

3.2.5. destroys or, where applicable, returns to the Data Controller, at the Data Controller's discretion, the data media containing personal and health data after the service has been provided, unless EU or Member State law requires the storage of personal data,

3.2.6. provides the Data Controller with all information necessary to verify the fulfilment of its obligations under this contract and to enable and facilitate audits, including on-site inspections, carried out by the Data Controller

3.2.7. declares that it does not use any decision making based on automated data processing, including profiling.

3.2.8. assists the Data Controller in fulfilling its obligations under Articles 32-36 of Section 2 of the GDPR, taking into account the nature of the processing and the information available to the Data Processor,

3.2.9. keeps records of data processing in accordance with Article 30(2) of the GDPR, keeps them updated and makes them available to the Data Controller.

3.2.10. shall inform the Data Controller without undue delay, but no later than within 1 (one) working day, if it believes that any of its instructions violate the provisions of the GDPR or the data protection provisions of a Member State or other EU data protection provisions.

3.3. The Data Processor is not obliged to verify whether the Data Controller has only allowed access to data the processing of which is indispensable for the performance of the Principal Agreement. The Data Processor shall not be under any additional processing obligation in relation to such data. Any liability in this regard shall be borne by the Data Controller.

3.4. The Data Processor shall forward to the Data Controller without delay, but no later than within 1 (one) day, any requests received in relation to Chapter III of the GDPR, supplemented with the information available.

4. Use of additional Data Processors

4.1. The Data Processor warrants that if, with the prior written consent of the Data Controller, it engages the services of an additional sub-processor, it will impose on such additional sub-processor the same data protection obligations as those set out in this Annex between the Data Controller and the Data Processor, in particular by providing the additional processor with appropriate guarantees to implement appropriate technical and organisational measures and thereby ensure that the processing complies with the requirements of the GDPR. If the additional processor fails to comply with its data protection obligations, the Data Processor shall be fully liable to the Data Controller for fulfilling the obligations of the additional data processor.

4.2. The Data Processor shall inform the Data Controller of any planned changes concerning the use or replacement of additional processors. The Data Processor shall act on the basis of the final decision communicated by the Data Controller regarding the use or replacement of additional data processors.

5. Data security

5.1. It is the sole responsibility of the Data Controller to design the processing operations in such a way as to ensure the protection of personal data when applying the GDPR, the Infotv. and other rules applicable to data processing.

5.2. It is the joint responsibility of the Data Controller and the Data Processor to provide the Data Processor with the technical and organisational measures which, having regard to the state of science and technology, the costs of implementation and the real risks to which the personal data to be processed are exposed, guarantee an adequate level of protection of the data, in particular in accordance with Article 32(1) of the GDPR.

6. Transfer of personal data

6.1. The parties mutually undertake to use the contact details of their contact persons for the purpose of data transmission in the course of contractual cooperation. The measures provided in the transfer procedure should ensure an adequate level of security, including confidentiality, taking into account the state of science and technology and the costs associated with the risks of implementation and the nature of the personal data to be protected.

6.2. When using a non-electronic (online) channel, when transmitting data on a data medium
6.2.1. take appropriate measures for the secure transmission of data media, and/or
6.2.2. are transmitted in an encrypted file on the medium, such that the password used for encryption is transmitted on a separate channel. In the case of transmission by open channels (e.g. by courier, post), the latter condition is mandatory.

6.3. The Data Processor declares that it will not transfer data to third countries or international organisations in the course of its activities.

6.4. If the need arises to transfer data to third countries or international organisations, the Data Processor shall inform the Data Controller in advance.

6.5. Data Processor may transfer data only with the prior written consent of the Data Controller.

7. Handling and reporting data breaches

7.1. The Data Processor undertakes to notify the Data Controller of any data breach of which it becomes aware in the course of contractual cooperation pursuant to Article 33(2) of the GDPR without undue delay after, and no later than 24 hours after becoming aware of it. The Data Processor shall endeavour to assist the Data Controller in making a notification under Article 33(3)(a) to (d) of the GDPR to the extent necessary and reasonable, but if the information is not fully available, the notification shall not be delayed and the additional information shall be provided as soon as it is available.

7.2. The Parties agree to communicate with the National Authority for Data Protection and Freedom of Information, as the supervisory authority of the Member State, through the Data Protection Officer of the Data Controller.