SALK
SALZBURGER LANDESKLINIKEN

DATA PROTECTION REGULATION

Agreement to Process Personal Data on behalf of the Controller

between

Gemeinnützige Salzburger Landeskliniken Betriebsgesellschaft mbH
Müllner Hauptstraße 48 | 5020 Salzburg
FN 240832s | VAT: ATU57476234

as Controller under Art. 4 No. 7 GDPR[1], hereinafter referred to as the **Controller**

and

HERE enter ... name as in the Commercial Register

HERE enter ... address and street number

HERE enter ... (country) postal code place

HERE enter ... Commercial Register number

as Processor under Art. 4 No. 8 GDPR, hereinafter referred to as the **"Processor"**, hereinafter referred to jointly as the "Parties" or each individually as a "Party".

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1 INTRODUCTION, SCOPE OF APPLICATION, DEFINITIONS

(1) The Controller and the Processor shall be in a contractual relationship.

(2) This Data Protection Agreement shall govern the rights and obligations of the Controller and the Processor under data protection law with respect to the processing of personal data.

(3) This Agreement shall apply to all processing activities involving personal data performed by the Processor, the Processor's employees or the sub-processors permissibly hired by the Processor (see Item 5 regarding sub-processors) on behalf of the Controller.

(4) The terms used in this Agreement shall be understood to have the same meanings as in the EU General Data Protection Regulation (GDPR)

(5) Supplements or amendments to this Data Protection Agreement must be in writing in accordance with § 886 of the Austrian Civil Code (ABGB).

2 SUBJECT MATTER TO BE PROCESSED

(1) The Processor shall perform the processing activities listed in Annex 1 for the purpose described therein.

(2) The Controller shall transfer the data listed in Annex 2 to the Processor, so it can perform the agreed-upon data processing activities.

3 THE PROCESSOR'S OBLIGATIONS

(1) To the extent that there is no express restriction to personal data below, the obligations of the Processor listed below shall refer to all data transmitted by the Controller, which the Processor may not dispose of or may not dispose of on its own.

(2) The Processor shall process personal data, including processing results, solely within the framework of the Controller's mandate and as contractually agreed. Therefore, the Processor may not use data provided to it for processing – or of which it has become aware – for any other purposes, especially for its own purposes, and shall only transmit said data to the agreed-upon recipient. If the Processor is or becomes required by law to process the Controller's data to an extent that goes beyond the documented instructions of the Controller pursuant to Art. 28 (3) lit a GDPR, the Processor shall verifiably inform the Controller before the processing takes place.

(3) The Processor agrees to maintain strict confidentiality with respect to all personal data and other information belonging to the Controller (such as business and trade secrets) of which it becomes aware within the context of the contractual relationship and to contractually impose this obligation on all persons who work for the Processor within the context of the mandate relationship[2], unless they are subject to an adequate statutory duty of confidentiality (Art. 28 (3) lit b GDPR and § 6 of the Austrian Data Protection Act (DSG) (2018)). This obligation shall also apply after the end of the Agreement and, for persons tasked with data processing, the obligation shall also continue after the end of their activities with the Processor or their departure from the Processor.

If there are doubts as to whether information is subject to a duty of non-disclosure, the information shall be treated as confidential until there is written authorization from the other Party.

(4) In connection with the processing assignment, the Processor shall assist the Controller in creating a record of processing activities (and updating it, if necessary) and conducting any necessary data protection impact assessment, giving due consideration to the information available to the Processor.

(5) The Processor may only provide information to data subjects and other third parties with the prior written consent of the Controller. The Processor shall promptly forward any direct inquiries it receives to the Controller to the extent that the inquiries relate to processing. The Processor shall meet the technical and organizational prerequisites so that the Controller can fulfill its obligation to handle requests related to protection of the rights of data subject in accordance with Chapter III of the GDPR (within the legal time limits) (Art. 28 (3) lit e GDPR).

(6) If the Controller is subjected to a review by supervisory authorities or other bodies authorized to do so or if data subjects assert their rights against the Controller, the Processor agrees to assist the Controller to the extent necessary, if the matter involves relevant processing activities.

(7) The data shall be processed solely within the EEA. The data may only be transferred to a third country with the written consent of the Controller and under the conditions set forth in Chapter V of the GDPR.

(8) If the Processor does not have a permanent establishment in the European Union, it shall appoint a responsible contact person in the European Union in accordance with Art. 27 GDPR. The contact data for the contact person and all changes in the identity of the contact person shall be promptly and verifiably reported to the Controller.

[2] The inclusion of such an obligation in the service agreement will be considered adequate as long as the obligation meets the minimum content requirements.

4 TECHNICAL AND ORGANIZATIONAL MEASURES

(1) The Processor agrees to take adequate (technical and organizational) security measures in accordance with Art. 32 GDPR and to always keep such measures state of the art to prevent the improper use of data or access to such data by unauthorized third parties.

(2) The Processor shall describe the security measures required by Art. 32 GDPR in a security concept, which shall take into account the minimum structures set forth in Annex 3, "Data security measures," and shall be updated to reflect the state of the art at regular intervals. The data security measures set forth therein shall be binding. They shall define the minimum requirements for the Processor. The Processor may not fall below this level.

(3) Upon request, the Processor shall prove to the Controller that it has met its obligations, particularly the obligation to fully implement the agreed-upon technical and organizational measures. The proof can be in the form of an approved code of conduct or a suitable, approved certification procedure.

(4) (Full or partial) copies of the Controller's databases may only be made if they are actually necessary to fulfill the mandate. All other copies shall require the verifiable approval of the Controller.

5 SUB-CONTRACTOR RELATIONSHIPS

(1) Sub-contractor relationships within the meaning of this Agreement only relate to those services that have a direct connection to the provision of the main service.

(2) The Processor may only hire additional processors (sub-processors) with the written consent of the Controller. The Processor must inform the Controller of its intention to hire a sub-processor in due time so that the Controller can prohibit this, if necessary, in accordance with Art. 28 (2) GDPR. In addition, the Processor shall ensure that the Controller can also give direct instructions to the sub-processor in accordance with the GDPR, if this is necessary from the perspective of data protection law.

(3) The Processor and the sub-processor shall agree in writing that the provisions of this Data Protection Agreement shall be binding on them (Art. 28 (4) GDPR). Upon request, the Controller shall be permitted to inspect the relevant contracts between the Processor and the sub-processor.

(4) The responsibilities of the Processor and the sub-processor must be clearly differentiated from each other.

(5) At the time of the signing of this Agreement, the sub-processors listed in Annex 4 "Approved sub-processors," together with their names, addresses and contract contents, have been assigned to process personal data of the scope indicated therein and have been approved by the Controller.

6 THE CONTROLLER'S RIGHTS AND OBLIGATIONS

(1) The Controller shall be entitled to reasonably verify the Processor's compliance with the data protection and data security provisions or to hire third parties to do so, particularly by obtaining information and inspecting the stored data and the data processing programs and to carry out any on-site controls.

(2) The Processor shall permit persons entrusted with control functions to be admitted and inspect, to the extent necessary and within the necessary scope, irrespective of possible business and trade secrets.

(3) The Processor shall provide the necessary information and demonstrate the processes and maintain the proofs necessary to perform checks.

(4) Controls with respect to the Processor shall be carried out without avoidable disruptions of the Processor's business operations. Checks shall be made after reasonable advance notice and during the Processor's regular business hours, unless otherwise required by urgent circumstances, documented by the Controller.

7 NOTIFICATION OBLIGATION

(1) In the event of a personal data breach, the Processor shall inform the Controller of this in a prompt and verifiable manner – at least within 24 hours after the Processor knew or should have known of the breach. In particular, breaches of data protection law or the provisions of this Data Protection Agreement by the Processor or its employees shall be promptly and verifiably reported.

(2) Reasonable suspicions must also be promptly reported.

(3) The notification must at least include the following information:

a) A description of the nature of the personal data breach, and, to the extent possible, information regarding the categories of data subjects and their approximate number and the categories of personal data records affected and their approximate number.

b) The name and contact details of the Processor´s data protection officer or other contact point where more information can be obtained.

c) A description of the probable consequences of the personal data breach.

d) A description of the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects (Art. 33 (2) and (3) GDPR).

(4) The Processor shall promptly inform the Controller of controls or measures of supervisory authorities or other third parties, to the extent that they relate to data processing.

(5) The Processor agrees to investigate every security incident and, together with the Controller, to take reasonable measures to safeguard the data and mitigate the possible adverse consequences for data subjects. In this regard, the Processor assures the Controller of its reasonable support in fulfilling its obligations under Arts. 33 and 34 GDPR.

(6) All obligations contained in this section shall also be imposed on any sub-processors.

8 END OF THE MANDATE

(1) At the end of the mandate relationship or at any other time, at the request of the Controller, the Processor shall, at the election of the Controller, either destroy the processed data or surrender the data to the Controller in a format designated by the Controller in accordance with Art. 4 No. 1 GDPR and confirm this. All existing copies of this data must also be destroyed. The data must be destroyed so that even residual information cannot be restored through reasonable effort. The nature and manner of destruction or surrender is set forth in binding detail in Annex 3, “Data security measures.” The destruction of the data must be verifiably confirmed to the Controller.

(2) The Processor shall also bring about or ensure the prompt return or documented destruction of such data by any sub-processors.

(3) The Processor shall retain documentation proving that the data were properly processed beyond the end of the Agreement in accordance with the relevant retention periods. At the end of the Agreement, the Processor can relieve itself of this obligation by surrendering the documentation of proper data processing to the Controller with the latter’s consent.

9 LIABILITY

The Processor shall be liable to compensate the losses suffered by the Controller due to the Processor’s or sub-processor’s personal data breaches or breaches of this Data Protection Agreement and shall indemnify the Controller and hold it harmless in this regard.

10 SPECIAL RIGHT OF TERMINATION

(1) The Controller can terminate contracts with the Processor at any time without a notice period (“special termination”) if the Processor or a sub-processor seriously violates data protection provisions or the provisions of this Data Protection Agreement with respect to a contract, or the Processor or a sub-processor rejects the Controller’s control rights in violation of the contract.

(2) A serious violation exists, in particular, if the Processor or a sub-processor does or did not substantially meet the obligations set forth in this Agreement, particularly with respect to the agreed-upon technical and organizational measures.

(3) For other violations of this Data Protection Agreement, the Controller shall allow the Processor a reasonable grace period to remedy the situation. If the Processor does not remedy the situation in due time, the Controller shall be entitled to terminate the contract without a notice period as described in this section.

(4) The Processor shall reimburse the Controller for all the costs associated with the premature termination of this Data Protection Agreement as the result of a justified exercise of this special right of termination.

11 MISCELLANEOUS

(1) Amendments or supplements to this Agreement must be in written form. There are no oral side agreements.

(2) If individual provisions of this Agreement are invalid, this shall not affect the validity of the Agreement in other respects.

(3) This Agreement will be construed, interpreted, governed and enforced in the laws of Austria without its conflict of law rules. The competent courts of Salzburg (City) shall have exclusive jurisdiction.

(4) In witness whereof, the Parties caused this Agreement to be executed in two counterparts by duly authorized representatives as of the Effective Date.

(5) This Data Protection Agreement supersedes any earlier data protection agreements.

12 SIGNATURES

.....	.....
Place, date	Place, date
.....	.....
Controller	Processor