SALK
SALZBURGER LANDESKLINIKEN

Annexes to the

DATA PROTECTION REGULATION

Agreement to Process Personal Data on behalf of the Controller

between

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

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

and

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).

A data protection agreement must be concluded for each processor. If a processor performs multiple processing activities, each of these must be documented in separate annexes. If an annex is subsequently added to the data protection agreement, it must be signed.

ANLAGE 1

To be filled out by the Processor

Identification of the processing activities and relevant systems, if any, and the purpose:
(e.g. KIS)

- ☐ **Remote access (SW fault analysis and debugging)**
- ☐ **Remote access (program maintenance, SW updates)**
- ☐ **SW fault analysis and on-site debugging**
- ☐ **Program maintenance/on-site installation of updates**
- ☐ **SW fault analysis for the Processor with respect to the data carrier provided**
- ☐ **Replacement of defective HW parts**
- ☐ **Elimination of malfunctions, restoration of the functionality of the HW**
- ☐ **Consulting services**
- ☐ **User training**
- ☐ **Help desk services**
- ☐ **System Administration**
- ☐ **Backup services**
- ☐ **Hosting services**
- ☐ **Other processing activities:**

Describe the processing activity accordingly on page 3.

Describe the processing activity: in shorthand form but with enough detail that an uninvolved third party can understand your statements, e.g. “Performance of payroll accounting” or “Operation of the Controller’s CRM system in the form of Software as a Service in the contractor’s computer center”

Brief description of the processing activity:
To be completed additionally by the processor

ANNEX 2

To be filled out by the Processor

Disclosed data

Please number the individual categories of data subjects consecutively. The respective number must later be assigned to the relevant data types and data transfer recipients.

Categories of data subjects: Data subjects affected (in the sphere of the Controller)

Number	Name

Data types: The following data types are being processed

Number	Name

Transfer of data: The Processor transfers (discloses) personal data to

Number	Name

Transfer of data to other EEA countries: The Processor transfers (discloses) personal data to

Nummer	Bezeichnung

ANNEX 3

Data security measures

The minimum technical and organizational measures to ensure data protection and data security, which the Processor must establish and maintain on an ongoing basis, are set forth below. Irrespective of the measures designated in Annex 3, security measures that have already been agreed upon in writing in underlying performance agreements, concepts or minutes, etc., shall remain valid. The goal is to ensure the confidentiality, integrity and availability, etc., of the information processed for the Controller.

Requirements for the Processor's security concept

1. Admission control (physical)

It must be ensured that unauthorized persons are denied admission to the ICT facilities in which personal data is processed and used, i.e. physical access to the ICT facilities must be regulated.

The following technical and organizational measures for the collection, processing and use of personal data by the Processor must be implemented in the agreed-upon basic contract:

1.1.	Measures for alerting personnel in critical areas are in place
1.2.	Measures for a manual locking system with arrangements for key management (key registration, key distribution system) are in place
1.3.	Measures for visitor registration are in place
1.4.	Measures for an electronic locking system with chip card/transponder for sensitive areas are in place
1.5.	Measures for the careful selection and instruction of cleaning personnel, building services personnel, … are in place

2. Access control (logical)

Use of data processing systems by unauthorized persons must be prevented, i.e. logical access to these ICT systems must be regulated.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

2.1.	Measures for authentication with user name/password (password issuance based on valid password rules) are in place
2.2.	Measures for the use of updated anti-virus software are in place
2.3.	Measures for the use of an updated firewall version on the perimeter and/or between other networks are in place (Standard: Everything that is not permitted is prohibited)
2.4.	Measures for the creation of user profiles are in place
2.5.	Measures for the encryption of mobile data carriers are in place
2.6.	Measures for the encryption of data carriers in laptops/notebooks are in place
2.7.	Measures for centralized smartphone management software (e.g. for the external erasure of data) are in place

3. User access control

It must be ensured that the person authorized to use a data processing system can only access the information in his respective user access area and that no personal data can be read, copied, changed or removed without appropriate authorization during the processing or use and after storage, i.e. authorization systems and information security measures must be developed.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

3.1.	Measures for the use of roles and authorizations based on the "need-to-know principle" are in place
3.2.	Measures to minimize the number of administrators (restriction to the "absolute minimum needed") are in place
3.3.	Measures to log user accesses to applications, entry, modification and erasure of data are in place
3.4.	Measures to securely erase data carriers before reuse are in place
3.5.	Measures for physical destruction (e.g., in accordance with DIN 66399) or hiring an appropriate service provider are in place
3.6.	Measures for the management of rights by specified system administrators and/or an identity management system with a defined process are in place
3.7.	Measures for a password guideline that defines the complexity, length and period of validity of the password or authentication using two factors and/or biometric methods are in place
3.8.	Measures to safely store data carriers based on the criticality of the data (lockable cabinets and drawers, data safe, …) are in place
3.9.	Measures to store the data in a secure place based on the classification of the data and/or its encryption are in place.

4. Transfer control

It must be ensured that no personal data can be read, copied, changed or removed by unauthorized persons during electronic transmission or storage on data carriers, and that it is possible to check and determine where personal data are to be sent, i.e., the method of data transmission must be regulated.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

4.1.	Measures for encryption during data transfer on the Internet or networks, which are not under sole control (e.g. TLS, …) by means of secure (state of the art) cryptographic procedures are in place
4.2.	Measures for the semi- or fully automatic identification of data recipients, for the semi- or fully automatic checking of the periods for scheduled transmissions and for the implementation of semi- or fully automatic erasure periods are in place

5. Input control

It must be ensured that it can be subsequently checked and determined whether and by whom personal data were entered into the data processing systems, changed or removed (e.g. by maintaining records).

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

5.1.	Measures for the logging of entries, changes or erasures of data are in place
5.2.	Measures to ensure the traceability of entries, changes or erasures of data by individual user names (not user groups) are in place
5.3.	Measures for the granting of rights to enter, change or erase data based on an authorization concept are in place
5.4.	Measures for the maintenance of overview lists, indicating which applications can be used to enter, change or erase data are in place

6. Availability control

It must be ensured that personal data are protected against inadvertent destruction or loss.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

6.1.	Measures for climate control in server rooms are in place
6.2.	Measures for equipment to monitor the temperature, humidity and other variables in server rooms are in place
6.3.	Measures for preventive fire protection (fire alarm systems) in server rooms are in place
6.4.	Measures for suitable fire extinguishers or extinguishing systems in server rooms are in place
6.5.	Measures for a backup and restoration concept are in place
6.6.	Measures for checking the restoration of data within a defined time frame are in place
6.7.	Suitable organizational measures for PATCH management are in place
6.8.	Measures for the storage of backed-up data in another fire compartment or in a secure external location are in place
6.9.	Measures to protect server rooms in flood zones are in place

7. Separation rule

It must be ensured that the data collected for different purposes are processed separately, i.e. there must be a functional separation or processing rights must only be assigned to the extent absolutely necessary (separation of duties). This rule shall also apply to administrators.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

7.1.	Measures for the establishment of database rights are in place
7.2.	Measures for the separation of user access rights for various clients are in place
7.3.	Measures for the separation of productive, quality and/or testing systems are in place

8. Emergency management

It must be ensured that there are suitable management processes in place for any personal data breaches that arise.

The following technical and organizational measures for the contractual collection, processing and use of personal data by the Processor must be implemented:

8.1.	Measures to identify, assess and eliminate personal data breaches are in place
8.2.	Measures to review the emergency process (e.g. audits, simulations, …) are in place

Security Measures after the end of the Agreement:

☐ Destruction of disclosed data

or

☐ surrender of the data to the Controller

ANNEX 4

To be filled out by the Processor

Sub-Processors

Minimum requirements: Name of the natural person or company name according to the commercial register, commercial register number, VAT number, country code, postal code, town, street/alley, outsourced processing activity