Contract number: [CONTRACT NUMBER]

DATA PROCESSING AGREEMENT - Agreement on the processing of personal data

Pursuant to Article 28 General Protection Regulation Article 4 (7) GDPR[1], (GDPR)

between

Wiener Gebietskrankenkasse, Wienerbergstraße 15–19, 1100 Wien

(„WGKK“) as the **„Controller“**,

and

[NAME OF THE LEGAL ENTITY, COMMERCIAL REGISTER, COMMERCIAL REGISTRATION NUMBER]

[UID NUMBER]

[ADDRESS]

As the „**Processor“** as defined in Article 4 (8) GDPR,

henceforth referred to as „parties“ or single „party“.

[1] 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 the Directive 95/46/EC (General Data Protection Regulation).

1 Introduction, Scope and Period of Validity, Definitions

(1) The Controller and Processor wish to record their commitments under this Agreement.

This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data Controller/Processor relationship under Data Protection Laws.

(2) The present Data Protection Agreement defines the rights and duties of both the Controller and the Processor to ensure data protection as stipulated in the context of the processing of personal data in this agreement.

(3) This agreement is undated/ is of unlimited validity for all data processing activities conducted by the Processor, employees of the Processor or hired sub-processors (cf. sub-contracting in chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**).

(4) The terms used in this agreement are in accordance with their usage and definitions as stated in the EU General Data Protection Regulation (GDPR).

2 Subject Matter

(1) The Processor adheres to the data protection criteria as detailed in

(2) Appendix 1.

(3) The Processor discloses to the Controller the personal data processed as detailed in

(4) Appendix 2.

3 Duties of the Processor

(1) Unless expressly limited to personal data in the following, the subsequent commitments of the Processor include all data transferred to the Processor by the Controller, for which the Processor is not or not solely in charge of.

(2) The Processor shall only process the data and utilize outcomes of the processing on the written instructions from WGKK and as detailed under this Agreement.

The processor shall not utilize the data received for processing for personal use or any purpose other than instructed by the Controller (WGKK). The Processor shall transfer the processed data exclusively to the Controller (WGKK).

The Processor shall provably inform the Controller if any processing of data should exceed the documented instructions as defined under the present agreement according to Article 28 para 3 (a) GDPR. This information shall be provided prior to engaging in processing activities exceeding the agreed processing activities.

(3) The Processor acknowledges the sensitive nature of data, including personal data and information on the Controller (such as trade or business secrets), and agrees to ensure the secure processing of data. The Processor further acknowledges to impose confidentiality commitments on all individuals who are concerned with the processing of data under the present agreement, particularly for individuals without duty of secrecy as detailed in Article 28 para 3 (b) GDPR and paragraph 6 DSG[2] (2018).

The commitment to confidentiality is undated and remains valid beyond the termination of the contract and conclusion of processing activities. In case of doubt as to whether information is subject to confidentiality, information shall be treated confidentially until confidentiality is lifted formally by the Controller.

(4) The Processor shall support the Controller in creating or updating the record of processing activities and in performing a potential data protection impact assessment with the data available to the Processor.

(5) The Processor shall provide information to the data subjects or other third parties exclusively after written consent by the Controller. The Processor shall immediately inform the Controller about any inquiries related to data processing that are directed at the Processor. The Processor shall provide the technical and organizational preconditions that allow the Processor to smoothly handle applications (within the legal deadline) concerning the exercise of the rights of the data subject in accordance with chapter III GDPR (Article 28 para 3 (e) GDPR).

(6) The Controller commits to supporting the Processor to the extent necessary in case of inspection by regulatory authorities or other authorized institutions or if data subjects assert rights against the Processor in the context of processing personal data.

(7) Data processing occurs exclusively in the European Economic Area (EEA). Any shift to a third country is only allowed by the Controller's written consent as detailed in the conditions under Appendix 2, chapter V GDPR.

(8) In case the Processor is not located in the European Union, the Processor shall appoint a responsible contact person according to Article 27 GDPR. The contact details of the appointed contact person as well as any changes regarding this contact person shall be communicated to the Controller immediately and demonstrably.

[2] Austrian Data Protection Act ("Datenschutzgesetz" 2018)

4 Technical and organizational measures

(1) The Processor commits to implementing adequate (technical and organizational) security measures in accordance with Article 32 GDPR. The Processor further agrees to staying up-to-date with the latest technology to avoid illegal use of data or a breach of contract, or to make data accessible to unauthorized third parties.

(2) The security measures envisaged in accordance with Article 32 GDPR may be implemented by means of an approved code of practice or rules of conduct, or by an adequate certification procedure – with evidence of the respective certificate (Appendix 3).

Without respective evidence, Appendix 3 (para 1-8) must be filled in correspondingly. The envisaged data security measures are legally binding. These must be updated regularly to keep up with the latest technological status. Since these serve as the Controller's minimum requirements, security measures must not fall below the minimum requirements.

(3) Upon request, the Processor shall provide proof to the Controller of the complete implementation of technical and organizational measures.

Partial or complete copies of the Controller's datasets may only be made if necessary for the fulfilment of the agreement. Any other copies require the Controller's provable explicit approval.

5 Sub-contracting

(1) Sub-contracts are defined as those services which have a direct connection to the main service provision.

(2) The hiring of an additional Processor (Sub-Processor) by the Processor is permissible only with the written consent of the Controller. Prior to hiring a Sub-Processor, the Processor is required to inform the Controller about the hiring intent of a Sub-Processor in due time so that the Controller may decline this intent in accordance with Article 28 para 2 GDPR. Moreover, the Processor shall ensure that the Controller be able to directly give GDPR-related instructions to the Sub-Processor if that were required by data protection measures.

(3) The liability regarding commitments and specifications of the present agreement shall be agreed on between Controller and Sub-Processor in written form (Article 28 para 4 GDPR). Upon request, the Controller shall be granted insight and access to view relevant contracts between the Processor and Sub-Processor.

(4) The responsibilities of the Processor and the Sub-Processor shall be clearly differentiated.

(5) At the time of contract conclusion, the Sub-Contractors listed in Appendix 2 (including name, address and details on the specified data processing activities) is officially approved by the Controller for the specified type and scope of processing personal data.

6 Rights and duties of the Controller

(1) The Controller has the right to personally inspect the Processor's compliance with provisions and instructions regarding the security and processing of personal data by requesting information, inspecting processed data and data processing systems, and by conducting on-site inspections. The Controller may commission a third party to conduct these inspections.

(2) The Processor agrees to allow the required access and insight to individuals commissioned by the Controller for inspection.

(3) The Processor commits to providing adequate information, demonstrating processes and delivering proof as required in the context of inspections.

(4) If possible, inspections at the Processor's site shall take place without avoidable disruption of normal conduct of business. If not specified otherwise, inspections occur at the Processor's business hours after giving sufficient prior notice. Urgent reasons with respective documentation on the part of the Controller may pose an exception.

7 Disclosure requirement

(1) The Processor shall inform the Controller immediately and demonstrably in case of a data security breach, i.e. no longer than 24 hours after the breach was recognized by the Processor. Particularly violations of data protection provisions by the Processor or Processor's employees must be communicated to the Controller provably and without delay.

(2) Justified suspicions must also be communicated without delay.

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

a) A description of the type of data breach, if possible with specification of the group and estimated number of data subjects, as well as the categories and estimated amount of the compromised data record.

b) The name and contact details of the Controller's data protection officer or any other point of contact for further information.

c) A description of potential consequences of the data breach.

d) A description of taken and recommended measures to remedy the data breach and, if necessary, measures to mitigate the potential negative effects (Article 33 para 2 and 3 GDPR).

(4) The Processor shall immediately inform the Controller about inspections or measures by regulatory authorities or other third parties in as far as these are related to data processing.

(5) The Processor commits to investigating each security incidence and to taking appropriate measures together with the Controller in order to secure the data and minimize potential negative consequences for the data subjects. The Processor assures to support the Controller in its duties to the extent required according to Article 33 and 34 GDPR.

(6) The entirety of duties contained in this article of the contract shall be imposed on potential Sub-Processors.

8 Termination of the Agreement

(1) At termination of the agreement or at instruction by the Controller, the Processor agrees to immediately return to the Controller all received and/or processed data in a specified format, or to delete the received and/or processed data. The Processor further agrees to provide proof to the Controller of the return or deletion of received and/or processed data. The return or deletion of data includes all copies of the data. The deletion shall occur in such a way that even the restoration of data with justifiable effort is no longer possible. The Processor shall provide proof of the deletion to the Controller.

(2) The Processor agrees to immediately return or provably delete data the Processor or Sub-Processor hold.

(3) The Processor agrees to maintain documentation serving as proof of the adequate processing of data for a determined period of time after termination of the agreement. If agreed upon with Controller, the Processor may hand over the documentation of adequate data processing to the Controller upon termination of the agreement.

9 Liability

The Processor is liable for compensation to the Controller resulting from GDPR infringements or breaches of the present agreement on the part of the Processor or Sub-Processor. The Controller consequently remains free from legal proceedings.

10 Extraordinary Termination

(1) The Controller may terminate all agreements with the Processor immediately ("extraordinary termination") in case of grave GDPR infringement, major breach of the present agreement or refusal of the Controller's right of control on the part of the Processor or Sub-Processor.

(2) An infringement is considered grave if the Processor or Sub-Processor significantly or completely fail to meet the commitments, particularly the agreed technical and organizational measures, detailed in this agreement.

(3) The Controller shall grant the Processor an adequate time frame to resolve other GDPR-related infringements. In case of non-timely remedial action, the Controller may resort to extraordinary termination (see paragraph 1).

(4) The Processor shall reimburse all costs to the Controller which arise from the premature termination of the present agreement due to extraordinary termination.

11 Other

(1) Changes or additions to the present agreement shall be made in written form. There are no verbal agreements.

(2) In case individual passages of the agreement are void, the rest of the agreement remains unaffected and thus vaild.

(3) The present data processing agreement substitutes all previous data processing agreements.

12 Signatures

Place, Date	Place, Date
.....	.....
Controller	Processor

Appendix 1

to [CONTRACT NUMBER] Description of the processing activity and, if applicable, relevant systems (e.g. ERP), including the purpose:

- ☐ **Remote Access (software error analysis and troubleshooting)**
- ☐ **Remote Access (maintenance of the program, software updates)**
- ☐ **Software error analysis and troubleshooting on site**
- ☐ **Maintenance of the program / installation of updates on site**
- ☐ **Software error analysis on behalf of the Processor due to handed over data carrier**
- ☐ **Exchange of defective hardware parts**
- ☐ **Elimination of malfunctions, restoration of hardware functionality**
- ☐ **Consulting services**
- ☐ **User training**
- ☐ **Helpdesk services**
- ☐ **Other processing activities ……..**

(Description of processing activities: in bullet points but with sufficient detail to allow uninvolved third parties to grasp the gist; for instance, “calculating pay slips” or “operating the CRM of the controller as software-as-a-service in the Controller’s computer centre”.)

Appendix 2

to [CONTRACT NUMBER]

Disclosed Data

(Please tick and add as applicable)

Categories of data subjects

The following entities or individuals are affected by data processing:

Applicants, employees, officials and functionaries (administration bodies and advisory board members), members of the supervisory authority of the Ministry of Finance (personnel data)	
Members of staff/contact persons of customers or suppliers of the Processor (recipients & providers of services or deliveries)	
Insured individuals, recipients of services	
Contracting partners (physicians, pharmacists, etc.), employer, representatives	
Patients	
Others: _____	

Data Types

The following types of data will be processed:

Identity data (such as names, academic degrees, birth dates, place of birth, date of death, sex, marital status, nationality, licence plate, parking space number, access area, etc.)	
Organisational or company data (such as head office, plant/company location, legal form, business branch, line of business/business section, economic class, professions, founding and wind-up information, dummy concern data, chamber membership, etc.).	
Contact information (such as address, drop-off points, electronic post box, telephone number, email address, IP address, fax number, etc.).	
Labour law related data, human resource & personnel management data (such as line of work, functions, education, length of service/insurance period, contribution base/basis for estimation, disability status, emoluments/earnings/salaries & wages, curia membership, union membership, employee provisions and pension fund data, social insurance body, application data etc.).	
Billing & payment data (such as bank data, credit transfer data, signature power, fee accounts, insolvency data, benefit statements, fees, charges & pay scale).	
Relatives or next of kin, agents, authorized persons, partnership, trustee, corporation, tenants, heirs, associates, partners, etc.	
Personal identification numbers (such as social security number, European health insurance card number, UID-, chamber membership number, commercial registration number, DRG Code, taxpayer identification number, etc.).	
Registration offices or report centres.	
Recourse data (e.g. data on the damaging party, damage, extent of damage, competent liability insurance, etc.).	
Contract-related data (e.g. time frame, specialization, qualifications, licenses, quotations,	

discounts, etc.).	
Patient data (e.g. service provider, date of death (these are included above in the identification data), institution, patient history, health state, medical indication, etc.).	
Other: _____	

Transmission and disclosure of data to Sub-Processors

In case of transmission and disclosure of personal data on behalf of the Processor (Name/designation, contact details, contract details):

Transmission of data to the EEA Area

In case of transmission and disclosure of personal data on behalf of the Processor (including remote access/service desk services):

Name & Details

Appendix 3

to [CONTRACT NUMBER]

Evidence of existing suitable technical & organizational measures for data protection is provided below:

Adherence to approved standard of behaviour according to Article 40 GDPR is available. Details:	
A certification based on a recognized certification process according to Article 42 GDPR is available. Details:	
Latest attestations and (partial) official reports of independent entities in accordance with common standards are available (e.g. certified public accountants, external data protection auditors, quality auditors) Details:	
A standardized certification by IT security or data protection audits (e.g. Baseline Protection of the Federal Office for Information Security, ISO 27001) is available. Details: The relevant certification details are to be added to Appendix 3a.	
Other detailed description of data protection measures in place (e.g. links on website): LINK:	

In case none of the above stated evidence is provided or any of the information provided above is not accepted by the Controller, the following questions need to be answered:

1. Access control (physical)

The Processor shall ensure that unauthorized individuals are denied access to IT systems, in which personal data are processed or used, i.e. the physical access to such IT systems must be regulated correspondingly.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
1.1	☐	☐	☐	Measures for alarms and alerts in critical areas are in place
	Grounds:			
1.2	☐	☐	☐	Measures for a manual locker system with clear rules for key management (key use registration, key distribution policy) are in place
	Grounds:			
1.3	☐	☐	☐	Measures for visitor registration are in place
	Grounds:			
1.4	☐	☐	☐	Measures for electronic locking systems with chip cards or transponders for high-security areas are in place

	Grounds:			
1.5	☐	☐	☐	Measures for careful selection and training of cleaning personnel, maintenance staff etc. are in place
	Grounds:			

2. Access control (logical)

The utilization of data processing system/equipment by unauthorized individuals must be prevented, i.e. the logical access to these IT systems must be properly regulated.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
2.1	☐	☐	☐	Measures for the authentication via user name and password (passwords based on secure, valid password rules) are in place
	Grounds:			
2.2	☐	☐	☐	Measures for the implementation of latest anti-virus and anti-malware software are in place
	Grounds:			
2.3	☐	☐	☐	Measures for the implementation of latest firewall versions on the perimeter and/or between other networks are in place (general rule: everything that is forbidden is not allowed)
	Grounds:			
2.4	☐	☐	☐	Measures for creating user profiles are in place
	Grounds:			
2.5	☐	☐	☐	Measures for the encryption of mobile data carriers are in place
	Grounds:			
2.6	☐	☐	☐	Measures for the encryption of data carriers in laptops and notebooks are in place
	Grounds:			
2.7	☐	☐	☐	Measures for a central smartphone administration software (e.g. for external deletion of data) is in place

	Grounds:	

3. Access control

The Processor shall ensure that authorized individuals are only granted access to data processing systems and information corresponding to their individual access authorization. The Processor shall further ensure that, during processing or utilization, no personal data be accessed, read, copied, changed, deleted or otherwise processed without corresponding authorization; i.e. permission systems and information security measures must be developed and implemented.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
3.1	☐	☐	☐	Measures for the implementation of role-based permissions (according to the "need-to-know principle") are in place
	Grounds:			
3.2	☐	☐	☐	Measures for the minimization of administrator accounts (limited to the „absolutely necessary minimum") are in place
	Grounds:			
3.3	☐	☐	☐	Measures for logging all access attempts to applications, as well as attempts to to enter, change or delete data are in place
	Grounds:			
3.4	☐	☐	☐	Measures for the secure deletion of data carriers prior to further usage are in place
	Grounds:			
3.5	☐	☐	☐	Measures for the physical destruction (e.g. according to DIN 66399) or commissioning of a respective service provider are in place
	Grounds:			
3.6	☐	☐	☐	Measures for the administration of rights and permissions by pre-defined/purported system administrators and/or an identity management system with a defined process are in place
	Grounds:			
3.7	☐	☐	☐	Measures for password guidelines detailing the complexity, the length, the validity as well as a two-factor authentication and/or biometric methods are in place
	Grounds:			

3.8	☐	☐	☐	Measures for the safekeeping of data carriers (e.g. lockers, lockable drawers, data safe, …) according to the level of criticality of saved data are in place
	Grounds:			
3.9	☐	☐	☐	Measures for storing data in a secure location according to the classification of data and/or their encryption are in place
	Grounds:			

4. Managing transfer of possession

During electronic transfer or storage of personal data, the Processor shall ensure that personal data cannot be read, copied, changed or deleted by unauthorized individuals. The Processor shall further ensure the possibility to examine and determine where personal data are to be transferred; i.e. the modality of data transfer must be regulated.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
4.1	☐	☐	☐	Measures for secure data encryption (according to the latest standards) in case of data transfer via the internet or networks, which are not under the Processor's exclusive power of control (e.g. TLS, …) are in place.
	Grounds:			
4.2	☐	☐	☐	Measures for the (semi-) automatic identification of data recipients, for the semi- or fully automatic verification of periods for planned transfers, and for the implementation of agreed time limits for semi- or fully automated deletion are in place.
	Grounds:			

5. Input Control

The Processor shall ensure the possibility to retrospectively examine and determine if, and by whom, personal data was entered, changed or deleted in data processing systems, by means of logging of data, for instance.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
5.1	☐	☐	☐	Measures for logging of data entry, change, or deletion are in place
	Grounds:			

5.2	☐	☐	☐	Measures for monitoring and tracking of data entry, change, or deletion by individual users (not user groups) are in place
	Grounds:			
5.3	☐	☐	☐	Measures for allocating permissions to enter, change or delete data based on a permission system are in place
	Grounds:			
5.4	☐	☐	☐	Measures for maintaining an overview over which applications are used for what kind of data entry, change, or deletion are in place
	Grounds:			

6. Availability monitoring

The Processor shall ensure that personal data be protected from unintentional, accidental deletion or loss.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
6.1	☐	☐	☐	Measures for air-conditioning in server rooms are in place
	Grounds:			
6.2	☐	☐	☐	Measures and devices for controlling the temperature, humidity and other measurements in server rooms are in place
	Grounds:			
6.3	☐	☐	☐	Measures for preventive fire safety (fire alarm system) in server rooms are in place
	Grounds:			
6.4	☐	☐	☐	Measures for suitable fire extinguishers or automatic fire extinguishing systems in server rooms are in place
	Grounds:			
6.5	☐	☐	☐	Measures for back-up and restoration are in place
	Grounds:			

6.6	☐	☐	☐	Measures for controlling and verifying the restoration of data within a defined time frame are in place
	Grounds:			
6.7	☐	☐	☐	Measures for adequate organizational PATCH management are in place
	Grounds:			
6.8	☐	☐	☐	Measures for storing saved data in another fire section or in another secure, external location are in place
	Grounds:			
6.9	☐	☐	☐	Measures for the protection of server rooms from floods are in place
	Grounds:			

7. Separation rule

The Processor shall ensure that personal data collected for diverse purposes be separately processed. This also means that data can and must be deleted when the specified purpose of processing is no longer given.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
7.1	☐	☐	☐	Measures for defining database rights are in place
	Grounds:			
7.2	☐	☐	☐	Measures for the separation of access rights for diverse clients are in place
	Grounds:			
7.3	☐	☐	☐	Measures for separating productive, quality and/or test environments/systems are in place
	Grounds:			

8. Emergency management

The Processor shall ensure the availability of adequate processes to manage data breaches.

The Processor shall implement the following technical and organizational measures for the compliant recording, processing and utilization of personal data:

Nr.	YES	NO	Not necessary	Minimum protection level ensured through: (ATTENTION: If „NO“ or „Not necessary“ are selected, please state the grounds.)
8.1	☐	☐	☐	Measures for recognizing, evaluating and resolving data breaches are in place
	Grounds:			
8.2	☐	☐	☐	Measures for the inspection of an emergency process (e.g. audits, simulation, …) are in place
	Grounds:			