APPENDIX 2 to Contract for the Commissioned Processing of Personal Data

Technical and organisational measures in accordance with the new Section 64 (3) BDSG- *[Bundesdatenschutzgesetz - Federal Data Protection Act]*

The Processor (Processor) gives an assurance to the Controller (Controller) that it has taken the following technical and organisational measures under the new Section 64 (3) BDSG and the pertinent Annex:

1. Access control

Denial of access by unauthorised persons to processing facilities with which the processing is carried out.

The application servers of the Processor are hosted exclusively in the computer centres of the respective cloud services provider in the territory of the European Union; accordingly, the storage and processing of personal data is carried out exclusively in the territory of the EU. The physical access to the facilities with which personal data is processed is restricted by the respective cloud services provider exclusively to named authorised persons, so that unauthorised persons are denied access to IT systems and data processing facilities.

In the cloud, the Processor uses both *Platform as a Service (PaaS)* and also *Infrastructure as a Service (IaaS*).

For Platform as a Service (PaaS):

The cloud provider carries out regular system updates and provides patches on the underlying physical and virtual machines.

For Infrastructure as a Service (IaaS):

The Processor carries out regular OS updates and security updates on all virtual machines of the cloud IaaS.

Description of the access control system:

☒ Alarm system

☒ Automatic access control system

☒ Lock system with code lock

☐ Biometrical access barriers

☒ Photo-electric barriers / Motion sensors

☒ Protection of building shafts

☒ Chip card/Transponder lock system

☒ Manual lock system

☒ Video surveillance of the entrances

☒ Security locks

☒ Regulation of keys (Issue of keys etc.)

☒ Logging of visitors

☒ Careful selection of security staff

☒ Identity check by the porter / at reception

☒ Careful selection of cleaning personnel

☒ Duty to carry passes

2. Data media control

Prevention of the unauthorised reading, copying, altering or erasure of data carriers.

The data is stored in logical volumes; no physical transport of these volumes takes place since the application infrastructure is operated completely by the cloud services provider. For the connection from the office to the computer centre, a VPN connection is used (encryption: AES 256). The transmission of personal data between the back end and the user UI is carried out using an SSL encryption (minimum encryption allowed: TLS 1.0). The storage of non-encrypted personal data in separate application modules takes place in one pseudonymized form, so that the assignment of data to persons can only be made over the Reference IDs. The Processor's IT administrators have no access to stored personal data since the individual data sets are encrypted through the application logic and can only be decrypted again using the application logic.

Description of the data carrier control system:

☒ Management of the rights by the system administrator

☒ Number of administrators reduced to the "necessary minimum"

☒ Preparation of an authorisation concept

☒ Password guidelines, including password length, change of password

☒ Encryption of data carriers

☒ Physical erasure of data carriers prior to re-use

□ Use of document shredders and service providers (as far as possible with privacy seal)

☒ Forwarding of data in anonymised or pseudonymised form

□ In the case of physical transport: secure transport containers / packaging

□ In the case of physical transport: careful selection of transport personnel and vehicles

☒ Encryption / password protection of data carriers in laptops / notebooks

☒ Secure storage of data carriers

☒ Proper destruction of data carriers (DIN 32757)

□ Logging of the destruction

3. Storage control

Prevention of the unauthorised input of personal data and of the unauthorised perusal, alteration or erasure of stored personal data.

The issue and alteration of the access rights for the Processor's application administrators is carried out by the role and rights management in the application. The Processor's IT administrators have no access to stored personal data since the individual data sets are encrypted by the application logic and can only be decrypted once more by the application logic. The physical storage of the data is carried out in the cloud on the logical storage units, so that the data is thereby fragmented and split between several physical drives. For the purpose of reading, the data fragments will be recompiled by the software layers.

Description of the storage control system:

☒ Fragmentation of the data upon storage

☒ Authentication by user name / password

□ Authentication using biometric methods

☒ Encryption of data carriers

☒ Encryption/password protection of data carriers in laptops / notebooks

☒ Allocation of user profiles to clients

4. User control

Prevention of the use by unauthorised persons of automated processing systems with the aid of facilities for data transmission.

The Processor's IT infrastructure is located entirely in the cloud. The IT administrators only have access via personal asymmetrical RSA keys (2048 bits); the keys are additionally protected with individual passwords. The log-ins of the IT administrators on the servers are recorded. Each issue of or change to the access rights is made in accordance with a dual control principle and is recorded. The necessity for users to have access rights is regularly reviewed, every 90 days. The off-boarding process ensures that user accesses are promptly revoked when they leave the company. The user IDs are unambiguous and individual. The passwords have at least 8 characters and must contain numerals, special characters and also small and capital letters. The passwords must be changed after 90 days. In the password history, the last 6 passwords will be stored. Following an incorrect entry 3 times in a row, the account will be automatically blocked.

Description of the user control system:

☒ Allocation of user profiles to IT systems

☒ Administration of the rights by the system administrator

☒ Authentication by user name / password

☒ Password guidelines, including password length, change of password

☒ Logging of accesses to applications, in particular in connection with the input, alteration or erasure of data

☐ Authentication using biometric methods

☒ Use of VPN technology

☒ Use of antivirus software

5. Access control

Guarantee that the persons authorised to use an automated processing system only have access to the personal data covered by their access authorisation.

The monitoring of the authorisation concept at the application level is the responsibility of the Controller. The necessary UI for the management of the roles and the access rights will be provided by the Processor. Amendments are to be logged. The issue and alteration of the access rights for the Processor's application administrators will be carried out by the same role and rights management in the application.

Description of the access control system:

☒ Preparation of an authorisation concept

☒ Number of administrators reduced to the "necessary minimum "

☒ Logging of accesses to applications, in particular in relation to the input, alteration and erasure of data

☒ Management of the rights by application administrators

☒ Password guidelines, including password length, change of password

☒ Client separation

6. Transmission control

Guarantee that it is possible to check and establish to which points personal data is transferred or provided or can be transferred or provided with the aid of data transmission facilities.

No data is passed on, since the infrastructure is operated entirely at the cloud provider. For the connection from the office to the computer centre, a VPN connection is used (encryption: AES 256). The transmission of personal data between the back end and the user UI is carried out using an SSL encryption (minimum encryption allowed: TLS 1.0). The storage of non-encrypted personal data in separate application modules takes place in one pseudonymized form, so that the assignment of data to persons can only be made over the Reference IDs.

Description of the control of onward transmission:

☒ Provision of dedicated circuits and VPN tunnels

□ E-mail encryption

□ Documentation of the recipients of data and of the time periods of the planned provision and agreed erasure periods

☒ Forwarding of data in anonymised or pseudonymised form

□ Preparation of an overview of regular retrieval and transmission processes

7. Input control

Guarantee that it is retrospectively possible to investigate and ascertain which personal data has been entered or altered in automated processing systems at which time and by whom.

The alterations are logged in the same database in which the data to be altered is also stored. Thus, the same rules apply for the log data as for the data itself. The log files of the application servers do not leave the protected network and are erased after 30 days. Only the Processor's IT administrators have access to the protected network. Access is gained via the asymmetric RSA system with a 2048 bit key length (individual keys).

Description of the input control system:

☒ Logging of the entry, alteration and erasure of data

☒ Traceability of the entry, alteration or erasure of data through individual user names (not user groups)

☒ Grant of rights for the entry, alteration or erasure of data on the basis of an authorisation concept

□ Preparation of an overview showing which data can be entered, altered or erased using which applications

□ Retention of forms from which data has been transferred to automated processes

8. Transport control

Guarantee that the confidentiality and integrity of the data is protected both in the transmission of personal data and also in the transport of data carriers.

No data or data carriers are transported, since the infrastructure is operated entirely at the cloud services provider. For the connection from the office to the computer centre, a VPN connection is used (encryption: AES 256). The transmission of personal data between the back end and the user UI is carried out using an SSL encryption (minimum encryption allowed: TLS 1.0). The storage of non-encrypted personal data in separate application modules takes place in one pseudonymized form, so that the assignment of data to persons can only be made over the Reference IDs.

Description of the transport control system:

☒ Provision of dedicated circuits and VPN tunnels

□ E-mail encryption

□ In the case of physical transport: careful selection of transport personnel and vehicles

☒ Forwarding of data in anonymised or pseudonymised form

□ Preparation of an overview of regular retrieval and transmission processes

□ During the physical transport: secure transport containers / packaging

9. Recoverability

Guarantee that the systems used can be recovered in the event of any failure.

Regular back-ups of the data will be prepared. The back-ups will be stored in the same protected network in which the data itself is processed. The physical storage of the back-ups is carried out in the cloud environment on the dedicated logical storage units.

Description of the recoverability system:

☒ Uninterruptable power supply (UPS)

☒ Equipment for the monitoring of temperature and humidity in server rooms

☒ Fire and smoke alarm systems

☒ Alarm signal in the case of unauthorised access to server rooms

☒ Testing of data recovery

☒ Retention of data back-ups in separate logical storage units

☒ Air conditioning facilities in server rooms

☒ Protected multiple mains sockets in server rooms

□ Fire extinguishers in server rooms

☒ Preparation of a back-up & recovery concept

☒ Preparation of an emergency plan

☒ Server rooms not located below sanitary facilities

10. Reliability

Guarantee that all functions in the system are available and that any malfunctions arising are reported.

The IT infrastructure and the functionality of the application are permanently monitored at several levels. In the case of faults, qualified staff are alerted. Faults are remedied in accordance with the emergency plan.

Description of the reliability system:

☒ Monitoring of the IT infrastructure and of the application at several levels

☒ Alarm given by e-mails and SMS

☒ Preparation of an emergency plan

☒ Fire and smoke alarm systems

☒ Equipment for the monitoring of temperature and humidity in server rooms

☒ Server rooms not located under sanitary facilities

11. Data integrity

Guarantee that personal data stored cannot be damaged through malfunctions of the system.

In the application logic, extensive rules are implemented to check and guarantee the data integrity. In the database, data integrity is, inter alia, ensured through normalisation concepts and constraints.

Description of the data integrity system:

☒ Rules for verifying the data when entered and when any changes are made

☒ Data normalisation

☒ Constraints on database objects

12. Commission control

Guarantee that personal data which is processed in commission can only be processed in accordance with the instructions of the Controller.

The selection of sub-processors is to be made with the greatest care; the processing of the data is carried out on the basis of the contract with the Processor in accordance with Art. 28 General Data Protection Regulation.

Description of the commission control system:

☒ Selection of the Processor under aspects of care (in particular in relation to data security)

☒ Written instructions to the Processor (e.g. by data processing contract)

☒ Processor has appointed a data protection officer

☒ Effective control rights agreed vis-à-vis the Processor

☒ Previous examination of the security measures taken by the Processor and documentation of the same

☒ Imposition of an obligation on the staff of the Processor to observe data secrecy

☒ Destruction of data following the end of the commission must be ensured

☒ Ongoing monitoring of the Processor and its activities

13. Availability control

Guarantee that personal data is protected against destruction or loss.

The back-ups are stored in the same protected network in which the data is also processed. No data carriers leave the protected network. The physical storage of the data is carried out in the cloud on the logical storage units, so that the data is thereby fragmented and split between several physical drives. In the reading process, the data fragments are recompiled by the software layer. Only the Processor's IT administrators have access to the network. Access is gained through the asymmetric RSA system with a 2048 bit key length (individual keys).

Description of the availability control system:

☒ Uninterruptable power supply (UPS)

☒ Equipment for the monitoring of temperature and humidity in server rooms

☒ Fire and smoke alarm systems

☒ Alarm signal in the case of unauthorised access to server rooms

☒ Testing of data recovery

☒ Retention of data back-ups at a secure, out-sourced location

☒ Air conditioning facilities in server rooms

☒ Protected multiple mains sockets in server rooms

□ Fire extinguishers in server rooms

☒ Preparation of a back-up & recovery concept

☒ Preparation of an emergency plan

☒ Server rooms not located below sanitary facilities

14. Separability

Guarantee that personal data collected for different purposes can be processed separately.

When storing the customer data, logical client separation applies; in the processing of this data, physical client separation applies. Productive and test systems are physically separated from each other. The storage of non-encrypted personal data in separate application modules takes place in one pseudonymized form, so that the assignment of data to persons can only be made over the Reference IDs.

Description of the separability system:

☐ Physically separate storage on separate systems or data carriers

☒ Preparation of an authorisation concept

☐ Provision of the data sets with purpose attributes / data fields

☒ Determination of database rights

☒ Logical client separation (by the software)

☐ Encryption of data sets which are processed for the same purpose

☐ In the case of pseudonymised data: Separation of the allocation file and storage on a separate, secured IT system

☒ Separation of productive and test systems