Contract for the Commissioned Processing of Personal Data pursuant to Art. 28 General Data Protection Regulation

Between

the **Controller**

and

Ingenious Technologies AG
Französische Str. 48
10117 Berlin
Germany

- hereinafter called the **Processor** –

1. Object of the Contract

(1) Within the scope of the use of the Ingenious technology pursuant to the General Terms and Conditions of Business of Ingenious (hereinafter the "Main Contract") it is necessary for the Processor to store and process data which is collected by the Controller in the course of the use of the Ingenious technology. It cannot be ruled out that this data represents personal data within the meaning of Art. 4, no. 1, GDPR. This Commissioned Data Processing Agreement applies exclusively for this data (hereinafter "Controller Data").

(2) This Contract sets out in concrete terms the rights and duties of the parties in relation to data protection in connection with the handling of the Controller Data by the Processor in the performance of the Main Contract.

2. Nature, scope, purpose and term of the commissioned processing

(1) The Processor will process the Controller Data on behalf of and in accordance with the instructions of the Controller within the meaning of Art. 28 GDPR (Commissioned Processing). The Controller remains the responsible body within the meaning of the data protection provisions in accordance with Art. 4, no. 7, GDPR.

(2) The processing of the Controller Data within the scope of the Commissioned Processing will be carried out in accordance with the stipulations concerning the nature, scope and purpose of the data processing contained in Annex 1 to this Contract. This relates to the nature of the Controller Data in Annex 1, the purpose of the data processing and the circle of data subjects specified there.

(3) The Controller Data will be processed in the territory of the Federal Republic of Germany, in any other member state of the European Union or in any other contracting state to the Agreement on the European Economic Area. Any transfer to a third country shall require the prior consent of the Controller and may only take place if the special conditions of Art. 44 et seq. GDPR are fulfilled.

(4) The term and termination of this Contract shall be governed by the provisions concerning the term and termination of the Main Contract. Any termination of the Main Contract automatically has the effect of terminating this Contract. A termination of this Contract in isolation is precluded.

3. Powers of the Controller to issue instructions

(1) The Controller Data will be handled by the Processor exclusively within the scope of the agreements made and in accordance with documented instructions of the Controller pursuant to Art. 28, para. 3, sentence 2 (a) GDPR unless the Processor is obliged to process the same in accordance with Union or Member State law to

which it is subject. In such a case, the Processor will inform the responsible officer of these legal requirements before carrying out the processing, unless that law prohibits the provision of such information on important grounds of public interest.

(2) Within the scope of the commission description set out in this Agreement, the Controller reserves the right to issue instructions relating to the nature, scope, means and purposes of the data processing, which it may specify in more detail through individual instructions. Should the Controller issue individual instructions in relation to the handling of Controller Data which go above and beyond the contractually agreed scope of performance, the costs thereby incurred are to be borne by the Controller.

(3) Any changes to the subject-matter of the processing or any changes in processes are to be jointly agreed and documented. The Processor may only provide information to third parties or to the data subject following the prior written consent of the Controller. The Processor is not entitled to pass on Controller Data to third parties and shall use the data for no other purposes, in particular not for its own purposes.

(4) The Processor is under no obligation to check the legitimacy of the instructions of the Controller under legal (data protection) provisions. The Processor shall immediately inform the Controller pursuant to Art. 28, para. 3, sentence 3, GDPR if, in its opinion, an instruction issued by the Controller infringes legal provisions. The Processor shall be entitled to suspend the implementation of the corresponding instruction until it has been confirmed or amended by the responsible officer at the Controller.

4. Duties of the Controller

(1) The Controller alone is responsible for the lawfulness of the data processing by the Processor and also for safeguarding the rights of the data subjects, and is thus the "controller" within the meaning of Art. 4, no. 7, GDPR.

(2) The Controller is the proprietor of all and any rights relating to the Controller Data.

(3) The Controller shall immediately inform the Processor if it discovers any errors or irregularities in connection with the processing of Controller Data by the Processor.

(4) Should any third parties assert claims against the Processor on account of the processing of Controller Data, the Controller shall indemnify the Processor from all such claims upon first demand.

5. Duties of the Processor

(1) The Processor shall ensure and regularly check that the processing of the Controller Data within the scope of the provision of services under the Main Contract in its area of responsibility, which includes the sub-contractors under Clause 9 of this Contract, is carried out in compliance with the provisions of this Contract.

(2) The Processor has appointed the data protection officer

Walter Meng,
Ingenious Technologies AG, Französische Straße 48, 10117 Berlin.

The Processor must inform the Controller immediately in the event of a change of the data protection officer.

(3) Pursuant to Art. 28, para. 3, sentence 2 (b), GDPR, the Processor shall impose an obligation of data secrecy by written agreement on all persons authorised to access personal data of the Controller, and shall advise them of the particular data protection obligations arising from this commission and also of the existing commitment to observe instructions and of the restriction to the specified purpose.

(4) Without the prior consent of the Controller, the Processor may not make any copies or duplicates of Controller Data within the scope of the Commissioned Processing. However, excepted herefrom are copies which are necessary in order to ensure orderly data processing and the orderly provision of services in accordance with the Main Contract (including data back-ups), and also copies which are necessary to comply with statutory obligations of retention.

(5) The Processor is obliged to support the Controller, within the reasonable and necessary limits and against reimbursement of the expenses and costs incurred as a result, in fulfilling his obligations under Article 12 to 22 and Article 32 to 36 GDPR. Support shall be provided taking into account the type of processing and the information available to the Processor as well as, where possible, appropriate technical and organisational measures, in particular in response to requests to exercise the rights of the data subject specified in Articles 12 to 22 GDPR.

Ingenious Technologies AG	**Executive Board**	**Supervisory Board**	**Amtsgericht Charlottenburg**	**Banking details**
Französische Str. 48	Dr. Siamak Haschemi	Mario Brockmann	HRB 160612 B	Commerzbank AG
10117 Berlin	Christian Kleinsorge	(Chairman)	Tax No.30/067/82795	IBAN DE29 7008 0000 0409 8547 00
Germany		Malte von der Ropp	VAT ID: DE814087813	
		Rene´ Bernebee´-Say		BIC DRESDEFF700

(6) The Processor shall be obliged to provide the Controller with all necessary information, including certifications and the results of reviews and inspections, which serve as documentary proof of compliance with the duties laid down in this Contract.

6. Technical and organisational measures

(1) Before beginning with the processing of the Controller Data, the Processor shall implement the technical and organisational measures listed in Annex 2 of this Contract and maintain the same in force during the term of the Contract.

(2) Since the technical and organisational measures will be governed by technical progress and further technological development, the Processor is permitted to implement alternative and adequate measures, provided that the level of security does not fall below the measures stipulated in Annex 2. The Processor is to document any such changes. Significant changes to the measures require the prior consent of the Controller and are to be documented by the Processor and provided to the Controller upon request.

7. Reportable breaches by the Processor

(1) The Processor shall inform the Controller promptly if it discovers that it or any employee has contravened data protection provisions or stipulations under this Contract in processing the Controller Data where the risk exists of a breach of the personal data of the Controller within the meaning of Art. 4, no. 12, GDPR.

(2) Where the Controller is under a statutory duty to provide information following an incident under para. (1) on account of an unlawful disclosure of Controller Data (in particular under Arts. 33 and 34 GDPR), the Processor shall, at the request of the Controller, support the latter, within the scope of that which is conscionable and necessary, in fulfilling its duties of providing information, subject to reimbursement of the expenses and costs thereby incurred by the Processor.

8. Control rights of the Controller

(1) Prior to the commencement of the data processing and then at regular intervals, the Controller shall, at its own expense, satisfy itself of the technical and organisational measures taken by the Processor in accordance with Annex 2, and shall document the result. For this purpose, it may obtain information from the Processor itself, request the submission of an attestation from an expert or, following the agreement of an appointment upon due notice, satisfy itself personally, without disrupting business operations and subject to observing strict secrecy in relation to industrial and business secrets of the Processor. The Processor undertakes to support the inspections of the Controller in an appropriate manner and to tolerate all necessary control measures.

(2) The Processor undertakes upon the written request of the Controller to give the latter, within a reasonable period, all information necessary for carrying out an inspection.

(3) The Processor shall at its own discretion be entitled, having consideration for the statutory obligations of the Controller, to withhold information which is sensitive in regard to the business of the Processor, or if the Processor would contravene statutory or other contractual provisions through disclosure of such information. The Controller shall not be entitled to be granted access to data or information about other customers of the Processor, to information relating to costs, quality control and contract management reports or to any other confidential data of the Processor which is not directly relevant for the agreed control purposes.

(4) The Controller shall inform the Processor in due time (as a rule, at least two weeks beforehand) of all circumstances relating to the performance of the inspection. As a rule, the Controller may perform one inspection per calendar year. The right of the Controller to carry out further inspections in the case of special incidents remains unaffected hereby.

(5) Should the Controller instruct a third party to perform the inspection, the Controller shall, by written agreement, impose the same obligations on the third party as the Controller itself has towards the Processor under this Clause 8 of this Contract. The Controller shall furthermore impose an obligation of confidentiality and secrecy on the third party unless the third party is bound by a duty of professional secrecy. At the request of the Processor, the Controller shall promptly submit to the Processor the agreements made with the third party containing these commitments. The Controller may not instruct any competitor of the Processor to carry out the inspection.

(6) At the option of the Processor, the documentary proof of compliance with the technical and organisational measures in accordance with Annex 2 may also, instead of an on-the-spot inspection, be provided through the submission of a suitable current attestation, of reports or extracts from reports of independent bodies (e.g. of certified public accountants, auditors, data protection officers, an IT security department, data protection auditors or quality auditors) or a suitable certification through an IT security or data protection audit - e.g. under BSI baseline protection *[baseline protection issued by the German Federal Office for Information Security]* - ("Audit Report"), provided the audit report enables the Controller to satisfy itself in an appropriate manner of compliance with the technical and organisational measures in accordance with Annex 2 to this Contract.

9. Sub-contracting

(1) The Processor may only establish subcontractor relationships in regard to the processing of Controller Data following the prior written consent of the Controller. Such prior consent may only be refused by the Controller for cogent reasons, of which evidence is to be produced to the Processor. The Processor will, upon request, deliver to the Controller an up-to-date overview of the sub-processors involved. Where written authorisation has been granted, the Processor will always inform the Controller of any intended change in regard to the enlistment or replacement of other processors.

(2) The Sub-Processors named in Annex 3 are deemed as approved by the Controller.

(3) In the event of the enlistment of a sub-processor, the Processor shall, by contract or any other legal instrument under European Union law or the law of the relevant member state, impose the same data protection obligations upon the sub-processor as are stipulated in this Contract. Should a sub-processor fail to fulfil the obligations stipulated in this Contract or contravene any data protection provisions, the Processor shall be liable to the Controller for compliance with the obligations of the sub-processor.

(4) Services of which the Processor avails itself from third parties as an ancillary service for the purpose of support in the performance of the commission are not understood to be sub-contractor relationships within the meaning of this provision and thus do not require the consent of the Controller. These include, in particular, telecommunications services, security services, maintenance and user service, cleaning personnel, auditors and the disposal of data carriers. However, in order to ensure the protection and security of the data of the Controller, the Processor shall, also in the case of outsourced ancillary services, be obliged to enter into contractual agreements in conformity with the law and to implement control measures.

10. Rights of the data subjects

(1) The rights of persons affected by the data processing are to be asserted against the Controller.

(2) Should a data subject apply directly to the Processor to protect his rights pertaining to personal data in accordance with Arts. 12 to 22 GDPR, the Processor will refer the data subject to the Controller.

(3) In the event that a data subject asserts his rights under Arts. 12 to 22 GDPR, the Processor shall support the Controller in satisfying these claims within a reasonable scope and within the scope necessary for the Controller in so far as the Controller is unable to satisfy the claims without the cooperation of the Processor. The Controller shall reimburse the Processor for any additional expenditure.

(4) The Processor shall enable the Controller to rectify, erase or block Controller Data or, at the request of the Controller, shall carry out the rectification, blockage or erasure itself if and in so far as the Controller is unable to do so itself.

11. Return and erasure of the Controller Data provided

(1) Following the end of the provision of services covered by the Contract (in particular in the case of termination or any other ending of the Main Contract) the Processor shall, at the option of the Controller, return or erase all Controller Data and destroy any existing copies, except where an obligation to store the data exists under a legal provision.

(5) The Processor shall prepare a protocol of the erasure or destruction of the Controller Data and provide the same to the Controller upon request.

(6) Documentation which serves as documentary proof of the orderly data processing in accordance with the terms of the commission or which is to be retained for the statutory retention periods is to be stored by the Processor beyond the end of the Contract in compliance with the respective retention periods.

12. Relationship to the Main Contract

Except where special provisions are contained in this Contract, the provisions of the Main Contract shall apply. In the event of any discrepancies between this Contract and provisions under other agreements, in particular under the Main Contract, the provisions of this Contract shall take precedence in so far as the processing of Controller Data is concerned.

______________________________ ______________________________

Place, date Place, date

______________________________ ______________________________

Controller Processor

APPENDIX 1 to Contract for the Commissioned Processing of Personal Data
Controller Data

Nature of the data	Purpose of collection of the data	Circle of data subjects
Person's Surname	Contract care, communication	Clients (Contact persons)
Person's First Name	Contract care, communication	Clients (Contact persons)
Telephone Number (business)	Contract care, communication	Clients (Contact persons)
Fax Number (business)	Contract care, communication	Clients (Contact persons)
Address (business)	Contract care, communication	Clients (Contact persons))
E-mail Address (business)	Contract care, communication	Clients (Contact persons)
Skype Address (Messenger)	Contract care, communication	Clients (Contact persons)
IP Address	Product functionality (Session management in the UI)	Clients (Staff)
Cookie ID	Product functionality (Session management in the UI)	Clients (Staff)
Person's Surname	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)

Person's First Name	Product functionality (Administration of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Date of Birth	Product functionality (Administration of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Telephone Number (business)	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Fax Number (business)	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Address (business)	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
E-mail Address (business)	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Skype Address (Messenger)	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Website URL	Product functionality (Management of the partnerships)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
Invoice Address	Product functionality (Payment processes)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators

IBAN / Account Number & Bank Sort Code	Product functionality (Payment processes)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators
Tax Number and/or VAT Number	Product functionality (Payment processes)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators
Partner Billing Country	Product functionality (Payment processes)	Customers of the clients: Publishers
Tax Office	Product functionality (Payment processes)	Customers of the clients: Publishers
Account Holder	Product functionality (Payment processes)	Customers of the clients: Publishers
User ID	Product functionality (Management and recognition of users in the UI)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Contact persons)
IP Address	Product functionality (Session management in the UI)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Staff)
Cookie ID	Product functionality (Session management in the UI)	Customers of the clients: Advertisers, Publishers, Agencies, Portal operators (Staff)
Customer ID	Product functionality (Billing, Reporting, Recognition of returning visitors)	End consumer
Order ID	Product functionality (Billing, Reporting)	End consumer
IP Address (anonymized)	Product functionality (Recognition of returning visitors)	End consumer

Cookie ID	Product functionality (Recognition of returning visitors)	End consumer
User Agent	Product functionality (Recognition of returning visitors)	End consumer
Referrer URL	Product functionality (Recognition of returning visitors)	End consumer
View Cookie ID	Product functionality (Recognition of returning visitors)	End consumer
Click Cookie ID	Product functionality (Recognition of returning visitors)	End consumer
Conversion ID	Product functionality (Recognition of returning visitors, Reporting)	End consumer
Is Customer New	Product functionality (Reporting)	End consumer
Customer Gender	Product functionality (Reporting)	End consumer
Customer Age	Product functionality (Reporting)	End consumer
Customer Survey	Product functionality (Reporting)	End consumer
Conversion Click ID	Product functionality (Recognition of returning visitors)	End consumer

Start Conversion ID	Product functionality (Recognition of returning visitors)	End consumer
Basket Freeze Conversion ID	Product functionality (Recognition of returning visitors)	End consumer
User Journey	Product functionality (Recognition of returning visitors)	End consumer
HTTP Header	Product functionality (Recognition of returning visitors)	End consumer

APPENDIX 2 to Contract for the Commissioned Processing of Personal Data

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

☒ Regulation of keys (Issue of keys etc.)

☒ Logging of visitors

☒ Careful selection of security staff

☒ Protection of building shafts

☒ Chip card/Transponder lock system

☒ Manual lock system

☒ Video surveillance of the entrances

☒ Security locks

☒ 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 reuse

□ 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

☒ 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

☒ Administration of the rights by the system administrator

☐ 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

☐ Email 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
- ☐ Email 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:

- ☒ Uninterruptible 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:

☒ Uninterruptible 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

APPENDIX 3 to Contract for the Commissioned Processing of Personal Data Approved Sub-Processors

Sub-Processors	Contact Details
Google Ireland Ltd.	Gordon House Barrow St Dublin 4, Ireland
Microsoft Ireland Operations Ltd.	Atrium Building Block B Carmanhall Road Sandyford Industrial Estate Dublin 18, Ireland