Agreement on Commissioned Processing of Personal Data Pursuant to Art. 28 Para. 3 GDPR

1. Object

1. This Agreement sets out in more detail the data protection obligations pursuant to Article 28 GDPR arising from the main agreement (hereinafter also referred to as „Main Agreement") concluded between Ubirch GmbH, Im Mediapark 5, 50670 Cologne (hereinafter: „Contractor" or „UBIRCH") and its client (hereinafter also referred to as „Customer" or „Client"; both jointly also referred to as „Parties").
2. The Contractor shall provide services (**ESG Exchange Network**) for the Client on the basis of the Main Agreement concluded between the Parties and the GTC included therein. In doing so, the Contractor shall process personal data within the meaning of Article 4 No. 1 of the German Data Protection Act (GDPA) for the Client (hereinafter referred to as "Client Data") exclusively on behalf of and in accordance with the instructions of the Client. The framework and scope of the data processing are set out in the Main Agreement. The Client shall be responsible for assessing the permissibility of the data processing.
3. This Agreement specifies the rights and obligations of the Parties under data protection law in connection with the Contractor's handling of the Client's data in fulfillment of the Main Agreement.

2. Duration of Processing

1. The term and termination of this Agreement shall be governed by the provisions governing the term and termination of the Main Agreement. Termination of the Main Agreement shall automatically result in termination of this contract. An isolated termination of this contract is excluded.
2. The Customer may terminate the Main Agreement in whole or in part without notice if the Contractor fails to fulfill its obligations under this contract, violates provisions of the GDPR with intent or gross negligence or is unable or unwilling to carry out an instruction of the Customer. In the case of simple - i.e. neither intentional nor grossly negligent - violations, the Customer shall set the Contractor a reasonable deadline within which the Contractor can remedy the violation.

3. Scope, nature and purpose of the processing, categories and types of personal data, categories of data subjects

1. The Contractor shall process the Client Data exclusively on behalf of and in accordance with the documented instructions of Client. Client shall remain the responsible party within the meaning of Art. 4 No. 7 GDPR.
2. The processing of the Client Data within the scope of the commissioned processing shall be carried out in accordance with the specifications of the service description contained in Annex 1 to this Agreement. It refers to the defined categories and types of Client Data, the categories of data subjects and the purpose of the processing.

3. The processing of the Client Data takes place in the territory of the Federal Republic of Germany, in another member state of the European Union or in another state party to the Agreement on the European Economic Area. Any transfer to a third country may only take place if the special requirements of chapter V of the GDPR (Art. 44 et seq. GDPR) are met.

4. Rights and duties as well as powers of instruction of Client

1. Client shall be solely responsible for assessing the permissibility of the processing and for safeguarding the rights of the data subjects under Articles 12 to 22 of the GDPR.
2. The processing of the Client Data by Contractor under this Agreement shall be carried out exclusively in accordance with Client's instructions pursuant to Art. 28 para. 3 sentence 2 lit. a GDPR, unless Contractor is required to carry out further processing under the law of the European Union or the law of the Member State to which it is subject. In such a case, Contractor shall notify Client of these legal requirements, unless the relevant law prohibits such notification due to an important public interest.
3. Within the scope of the order description agreed in this Agreement, Customer reserves a comprehensive right to issue instructions regarding the type and purpose of the data processing, which it may specify by means of individual instructions.

5. individual instructions after conclusion of the contract require text form and are to be documented by both Parties.

1. The persons authorized to issue instructions and the recipients of instructions are shown in Annex 3. In the event of a change or a longer-term prevention of the persons named, the successor or representative must be named to the contracting party in text form without delay.
2. If Client issues individual instructions regarding the handling of Client Data that go beyond the scope of services agreed in the Main Agreement, the costs incurred as a result shall be borne by Client. Such instructions shall be treated as a request for a change in performance.
3. Contractor shall not be under any obligation to review Client's instructions in terms of (data protection) law. However, if Contractor is of the opinion that an instruction of Customer violates the provisions of data protection law, it shall point this out to Customer. Contractor shall be entitled to suspend the implementation of the relevant instruction until the instruction is confirmed or amended. If Customer does not dispel Contractor's concerns in response to the information about an instruction that is illegal in Contractor's opinion, Contractor may refuse to implement the instruction in question insofar as it affects his sphere of responsibility.
4. Customer shall inform Contractor immediately and in full if he discovers errors or irregularities in connection with the processing of Client Data by Contractor or his instructions.

6. Duties of Contractor

1. Contractor shall ensure that the processing of the Client Data within the scope of the provision of services under the Main Agreement in its area of responsibility, which includes the subcontractors under Section 9 of this Agreement, is carried out in accordance with the provisions of this Agreement.

2. Contractor shall be obliged to provide Contractor, upon request, with the necessary information, including certifications as well as audit and inspection results, which serve to prove compliance with the obligations set forth in this Agreement.

3. Contractor shall impose a written confidentiality obligation on the persons authorized to process Client Data pursuant to Art. 28 para. 3 lit. b GDPR, unless they are already subject to an appropriate statutory confidentiality obligation.

4. Contractor shall be obligated to appoint a competent and reliable data protection officer in writing who can perform his activities in accordance with Artt. 37, 38 and 39 GDPR as well as Section 38 BDSG, if and as long as the legal requirements for an obligation to appoint are met. Contractor shall make the current contact details of the data protection officer easily accessible on his website (Art. 37 para. 7 GDPR).

5. Contractor shall keep a register of processing activities relating to the Client Data, which shall contain all information pursuant to Art. 30 para. 2 GDPR. This obligation shall not apply if the requirements of Art. 30 para. 5 GDPR are met. The register shall be made available to Client upon request. Upon request, Contractor shall provide Customer with the respective information required for the latter's register of processing activities.

6. Contractor may not make copies or duplicates of the Client Data within the scope of the commissioned processing without the prior consent of Client. However, this shall not apply to copies to the extent that they are required to ensure proper data processing and proper provision of the services under the Main Agreement (including data backup), as well as copies required to comply with statutory retention obligations.

7. Contractor shall be obliged to support Client within the scope of what is reasonable and necessary and against reimbursement of the expenses and costs incurred by Contractor in fulfilling his obligations under Artt. 12 to 22 and Artt. 32 to 36 GDPR. The support shall be provided taking into account the type of processing and the information available to Contractor and, where possible, with appropriate technical and organizational measures, in particular in responding to requests to exercise the rights of the data subjects set out accordingly in Artt. 12 to 22 GDPR (Section 10).

7. Technical and organizational measures

1. Contractor shall take the necessary technical and organizational measures to adequately protect the Client Data pursuant to Art. 32 GDPR, in particular access control, authorization control, transfer control, input control, order control, availability control and separation control measures listed in Annex 4.

2. Since the technical and organizational measures are subject to technical progress and technological development, the Contractor shall be permitted to implement alternative and adequate measures for adaptation, provided that the security level of the measures specified in Annex 4 is not undercut in the process. Contractor shall document such changes. Significant changes to the measures require the prior consent of Customer.

8. Notification obligations of Contractor

1. In the event of disruptions, suspected data protection violations or violations of contractual obligations of Contractor, suspected security-related incidents or other irregularities in the processing of the Client Data by Contractor, persons employed by it within the scope of the contract or by third parties, Contractor shall inform Customer immediately in writing or text form. The same shall apply to audits of Contractor by the data protection supervisory

authority. The notification of a personal data breach shall contain at least the following information:

a. description of the nature of the personal data breach, including, to the extent possible, the categories and number of data subjects, the categories affected and the number of personal data records affected;

b. description of the measures taken or proposed by Contractor to address the breach and, where applicable, measures to mitigate its possible adverse effects.

2. Insofar as Customer is subject to statutory duties to provide information due to unlawful acquisition of Client Data (in particular pursuant to Artt. 33 and 34 GDPR) as a result of an incident pursuant to paragraph 1, Contractor shall support Customer in fulfilling the duties to provide information upon Customer's request within the scope of what is reasonable and necessary.

3. Contractor shall immediately take the necessary measures to secure the Client Data and to mitigate any possible adverse consequences for the data subjects, inform Client thereof and request further instructions.

4. Contractor may only carry out notifications pursuant to Artt. 33 or 34 GDPR for Client after prior instruction by Client.

5. Should the Client Data be endangered by seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties, Contractor shall inform Customer thereof without undue delay, unless he is prohibited from doing so by court or administrative order. In this context, Contractor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with Client as the responsible party within the meaning of the GDPR.

9. Client's rights to monitoring

1. Customer shall satisfy itself at its own expense of the technical and organizational measures of Contractor in accordance with Annex 4 prior to the commencement of data processing and thereafter on a regular basis and shall document the result. This shall be done by obtaining a self-disclosure from Contractor, which Contractor may also fulfill by submitting a suitable certificate from an expert.

2. Contractor undertakes to provide Customer, upon written request, with all necessary information and details regarding its obligations under this Agreement and, in particular, to provide evidence of the implementation of the technical and organizational measures set forth in Annex 4. The proof of such measures, which do not only concern the specific order, can be provided by compliance with approved rules of conduct pursuant to Art. 40 GDPR or certifications pursuant to Art. 42 GDPR, current test certificates, reports or report excerpts of independent bodies (e.g. auditors, auditing, data protection officer, IT security department, data protection auditors, quality auditors), a suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).

3. Customer or an appropriately authorized representative shall have the right to carry out the aforementioned checks during normal business hours. These inspections shall be announced in good time (as a rule at least two weeks in advance) and shall only interfere with Contractor's business operations as little as possible.

4. If Customer commissions a third party to carry out the inspection, Customer shall oblige the third party in writing in the same way as Customer is obliged under this contract. In addition, he shall oblige the third party to maintain secrecy and confidentiality, unless the third party is subject to a professional confidentiality obligation. Upon request of Contractor, Client shall

submit to Contractor the obligation agreements with the third party. Customer may not commission a competitor of Contractor with the inspection.

5. Customer shall document the results of the inspections and inform Contractor thereof. In the event of errors or irregularities discovered by Customer, in particular during the inspection of contract results, Customer shall inform Contractor without delay. If facts are discovered during the inspection, the future avoidance of which requires changes to the ordered procedure, Customer shall inform Contractor of the necessary procedural changes without delay.

10. Subcontracting

1. Customer expressly consents to the commissioning of the subcontractors listed in Annex 3 subject to the condition of a contractual agreement in accordance with Article 28 paras. 2 and 4 GDPR. Contractor is permitted to commission further subcontractors (further Processors).
2. Subcontractors within the meaning of this provision are service providers who are directly entrusted with the provision of the main service. The main service does not include ancillary services which Contractor uses e.g. as telecommunication services, postal/transport services, maintenance and user service or for the disposal of data storage containers as well as for other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.
3. Contractor shall inform Customer without delay of any intended change with regard to the use or replacement of other subcontractors. Customer may object to such changes for good cause to be proven to Contractor. The objection shall be made in writing within a period of one week from receipt of a corresponding notification from Contractor.
4. No notification shall be required for the involvement of subcontractors where the subcontractor merely provides an ancillary service to support the provision of services under the Main Agreement, e.g. as telecommunication services, postal/transport services, maintenance and user service or for the disposal of data storage containers as well as for other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems, even if access to Client Data cannot be excluded in the process. Contractor shall also select these with due care and enter into agreements to the extent necessary to ensure adequate protection of the Client Data.
5. In the event that a subcontractor is used, Contractor shall impose on the subcontractor, by way of a contract or other legal instrument under European Union law or the law of the member state concerned, the same data protection obligations as those set forth in this Agreement. The contract shall be structured in such a way that it is possible for Customer, if necessary, to carry out appropriate checks and inspections at the subcontractor's premises, also on site, or to have them carried out by third parties commissioned by Customer. Upon request, Contractor shall provide Customer with evidence of the conclusion of the aforementioned agreements with his subcontractors.
6. If subcontractors in a third country are to be involved, Contractor shall ensure that the requirements of chapter V of the GDPR (Art. 44 et seq. GDPR) are met.

11. Rights of data subjects

1. The rights of the data subjects affected by the data processing shall be asserted against Client.

2. Insofar as a data subject should contact Contractor directly in order to exercise his rights under Artt. 12 to 22 GDPR in respect of the personal data relating to him, Contractor shall refer the data subject to Client.

3. In all other respects, Section 5 (7) of this Agreement shall apply.

12. Liability

1. Customer and Contractor shall be jointly and severally liable for the compensation of damages suffered by a person due to unlawful or incorrect data processing within the scope of the contractual relationship.

2. Customer shall be solely responsible for the compensation of damages suffered by a data subject due to an inadmissible or incorrect processing of Client Data within the scope of the commissioned processing in accordance with the applicable data protection law in the internal relationship with Contractor.

3. Customer undertakes to indemnify Contractor in the internal relationship from all claims of third parties as long as and to the extent that it does not prove that Contractor has not complied with its obligations under the GDPR specifically incumbent on Contractor or has acted in non-compliance with a lawfully issued instruction of Customer or against a lawfully issued instruction.

4. If a data protection authority or a court imposes a fine on Contractor based on data processing by Contractor that is based on an instruction of Customer, Customer shall reimburse Contractor the corresponding amount in full upon written notice within 30 days of the written notice.

5. Customer shall reimburse Contractor for all costs resulting from the infringement for which Contractor is responsible pursuant to paragraphs (3) and (4), including the costs of legal proceedings.

6. Unlimited liability: Contractor shall be liable without limitation for intent and gross negligence, in the event of breach of a contractually granted warranty and in accordance with the Product Liability Act. Contractor shall be liable for slight negligence in the event of damage resulting from injury to life, body and health of persons. In all other respects, the following limited liability shall apply: In the event of slight negligence, Contractor shall only be liable in the event of a breach of a material contractual obligation under the Main Agreement, the fulfillment of which makes the proper performance of the Main Agreement possible in the first place and on the observance of which Customer may regularly rely (cardinal obligation). The liability for slight negligence is limited to the amount of the damages foreseeable at the time of conclusion of the contract, the occurrence of which must typically be expected in such cases.

13. Return and deletion of provided Client Data

1. Contractor shall return or delete all Client Data at the discretion of Customer after termination of the contractual performance (in particular in the event of termination or other termination of the Main Agreement) and destroy existing copies, unless there is an obligation to store the data under European Union law or the law of the member states.

2. Contractor shall prepare a record of any deletion or destruction of Client Data, which shall be submitted to Customer upon request.

3. Documentation which serves as proof of the proper processing of data in accordance with the order or statutory retention periods shall be retained by Contractor beyond the end of the contract in accordance with the respective retention periods.
4. Contractor shall be obligated to treat as confidential any Client Data of which he becomes aware in connection with the Main Agreement, even after the end of the Main Agreement. The present agreement shall remain valid beyond the end of the Main Agreement for as long as Contractor disposes of Client Data which have been forwarded to him by Client or which it has collected for Client.

14. Final provisions

1. The Parties undertake to treat as confidential the business secrets of the other party and all other information, in particular of a technical and commercial nature, intentions, experience, findings and documents, including those which become known to them as a result of the cooperation under this Agreement (together referred to as "Confidential Information"), not to make them accessible to third parties and to protect them from access by third parties, even beyond the term of the Agreement.
2. Insofar as no special provisions are contained in this Agreement, the provisions of the Main Agreement shall apply. In the event of contradictions between this Agreement and provisions from other agreements, in particular from the Main Agreement, the provisions from this Agreement shall take precedence.
3. Amendments or additions to this Agreement must be made in writing. This shall also apply to any waiver of this formal requirement.
4. Changes in the contact information of one party shall be notified to the other party without undue delay. The last known contact information shall apply until it is expressly updated.
5. If any provision of this Agreement is or becomes invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effect comes as close as possible to the objective pursued by the contracting parties with the invalid or unenforceable provision. The above provisions shall apply mutatis mutandis in the event that the agreement proves to be incomplete.
6. Customer and Contractor and, if applicable, their representatives shall cooperate with the supervisory authority in the performance of their duties upon request.
7. This Agreement shall be governed by German law. The exclusive place of jurisdiction is Cologne.

Annexes

Annes 1 Service Description

Annex 2 Instructors and Instructees

Annex 3 Permitted Subcontractors

Annex 4 Technical and Organizational Measures

This contract was accepted by the parties electronically and is therefore valid without signature.

Annex 1
Service Description

Contractor shall provide the data processing services listed in accordance with this Annex to Customer exclusively in accordance with the instructions and on behalf of Customer and on the basis of the order processing agreement concluded between the Parties.

Contractor shall process the following Customer Data on behalf of Customer for the aforementioned purposes:

Data Categories	Categories of data subjects	Purpose of data processing
Data related to the collection and disclosure of sustainability reports Identifiers, contact information, certifications, measurements, estimates, metrics	Customer and suppliers of customer	Collection, aggregation, disclosure, signing, and storage of customer reports and related data
User Profiles Name, Email Address, Address, Password	Customer and suppliers of customer	Management and use of the platform
Name, Email Address, Telephone Number	Customer and suppliers of customer	Contacting suppliers of a Customer for platform invitation on behalf of this Customer

Annex 2
Instructors and Instructees

Permitted to instruct on behalf of Client is/are the person(s) expressly designated by Client as authorized to issue instructions on behalf of Client. This designation should happen in written form (email is sufficient). If no person is expressly named or if the expressly named person is absent, any person who has access to the service within the meaning of the Main Agreement on the side of Client shall be authorized to issue instructions.

Responsible for the reception of instructions are:

- Matthias L. Jugel, CTO, matthias.jugel@ubirch.com, +49-30-95.99.96.501

In the event of a change or long-term prevention of the contact persons, the other party must be informed immediately and in principle in writing or electronically of the successors or the representatives. The instructions shall be retained for their period of validity and subsequently for three full calendar years.

Annex 3
Permitted Subcontractors

Name/company name of the subcontractor (incl. address)	Service	Third country transfer (yes/no) If yes: On what basis pursuant to Art. 44 et seq. GDPR
T-Systems International GmbH Hahnstraße 43d D-60528 Frankfurt am Main	Data center infrastructure	no
Gronemeyer IT GmbH Konrad-Zuse-Str. 1 37671 Höxter	File Sharing, Mail-Service	no
Atlassian. Pty Ltd Level 6, 341 George Street Sydney NSW 2000 Australien	Help Desk	yes
OpenAI, LLC C13473A10009 548 Market Street PMB 97273 San Francisco, California 941045401 United States	Support Chat/Help	Necessary for Contract Performance
Chatbase.co Inc. Address: 4700 Keele St, Toronto, ON M3J 1P3 Canada	Support Chat/Help	Yes, Necessary for Contract Performance
Pipedrive OU Mustamäe tee 3a Tallinn, Harjumaa 10615 Estonia	CRM	Yes, Necessary for Contract Performance

Annex 4
Technical and Organizational Measures

No. 5 of the Agreement on Commissioned Data Processing refers to this Annex for the specification of the technical and organizational measures (Hereinafter referred to as „TOMs"). In detail, the following measures are defined, which serve to implement the requirements of Article 32 of the GDPR:

Column A of the following chart (general TOMs): TOMs in this column marked with a check apply generally (incl. system area in the data center) at UBIRCH and are not limited to a specific system environment or a specialized procedure (e.g. by guidelines, ISO documents or service instructions).

I. Pseudonymization and Encryption (Art. 32 para. 1 lit. a GDPR)

Measure	A
Access to the company network only via encrypted tunnel	☒
Email encryption for employees using S/MIME encryption.	☒
E-mail encryption with OpenPGP: If required and the recipients are able to receive, e-mails are encrypted with openPGP	☒
Data is only passed on on data carriers or sent electronically in anonymized or pseudonymized form: Only completely anonymized data will be sent. The data stored in the procedure does not allow identification of natural persons.	☒
Smartphone content encryption: - Company smartphones are encrypted by default.	☒
Access restriction by end device: Critical endpoints are linked to personal accounts to restrict who can log in.	☒
File encryption: Files with personal information are always encrypted.	☒
Disk encryption: Disks are always encrypted using FileVault (Mac) or Bit-Locker (Windows) and FDE (Linux). Recovery codes are stored securely and separately from the encrypted disks.	☒

II. Confidentiality, integrity (Art. 32 para. 1 lit. b GDPR)

A. Authorization/access control

Denial of access to processing equipment to unauthorized persons with whom processing is performed.

Measure	A
Alarm system: Installed at location Cologne	☒
Fixed cleaning times: Fixed cleaning times are defined.	☒

Implementation of a role and authorization concept: • Access to audit logs • Administration No personal data is stored by the server (with the exception of the audit log).	☒
Individual user accounts: Each system user has an individual user account. Sharing user accounts is prohibited.	☒
Password policies appropriate to the purpose: A password policy with high security requirements is implemented technically. No personal data is stored by the server.	☒
Prevention of SQL-infections through • content filter for SQL-statements for input fields • object relational mappers • database restrictions (only registered host can execute database statements)	☒
Authentication with password+2FA: Employees authenticate themselves to the system via user name, password and second factor (Authenticator App)	☒
Regulations when employees leave the company: As part of the offboarding process, all accounts of the departing employee are deactivated.	☒
Account blocking after multiple incorrect password entries: The account will be blocked after multiple (six attempts) incorrect entry of user passwords.	☒
Assignment of user profiles to IT systems (Windows)	☒
Disk encryption: Disks are always encrypted using FileVault (Mac) or Bit-Locker (Windows). Recovery codes are stored securely and separately from the encrypted disks.	☒

B. Data storage control

Prevent unauthorized reading, copying, modification or deletion of data storage. In addition to preventing physical access to the data storage containers (above authorization/access control), the following measures are taken.

Measure	**A**
Secure deletion of data carriers: Data carriers are reliably deleted.	☒

C. Memory control

Measure	**A**
Assignment of administrator rights to a minimum number of persons: Administrator rights are limited to a minimum number of persons.	☒

D. Prevention of unauthorized entry of personal data as well as unauthorized knowledge, modification and deletion of stored personal data.

Measure	**A**
Management of rights by system administrator	☒

Password policy incl. password length, password change	☒
Logging of accesses to applications, especially during input, modification and deletion of data for production systems (server).	☒
Physical deletion of data carriers before reuse	☒
Use of document shredders or service providers (if possible with a data protection seal of approval)	☒
Encryption of data storage	☒
Creating user profiles	☒
Assignment of user profiles to IT systems	☒
Use of VPN technology	☒
Secure storage of data storage containers	☒

E. User control

Preventing the use of automated processing systems by unauthorized personnel using data transmission equipment.

Measure	**A**
Two-factor authentication	☒
Identity management system (SSO, IAM)	☒
Password policy incl. password length, password change	☒
Logging of access to applications, especially when entering, changing and deleting data: Implemented through audit log.	☒
Tiered authorization structures	☒
Demilitarized zone (DMZ) facility	☒
Certificates for VPN access	☒

F. Access control

Ensuring that those authorized to use an automated processing system have access only to the personal data covered by their access authorization.

Client separation: A logical client separation exists.	☒
Audit Log: An audit log records the issuance of certificates	☒
Pseudonymizing real data for developers	☒

G. Transmission control

Ensuring that it is possible to verify and identify where personal data has been or may be transmitted or made available using data transmission equipment.

Measure	**A**
Create an overview of regular retrieval and transmission operations	☒
PC: Firewall rules are implemented. Ubiquiti security gateway is used.	☒
End-to-end transport encryption for e-mail transmission: End-to-end transport encryption is ensured during e-mail transmission.	☒
Documentation of the recipients of data and the time periods of the planned transfer or agreed deletion periods	☒
In physical transport: careful selection of transport personnel and vehicles.	☒
Other type of logging (e.g., by recording on paper and archiving).	☒
Establishment of dedicated lines or VPN tunnels	☒
During physical transport: secure transport containers/packaging	☒

H. Input control

Ensuring that it is possible to check and determine retrospectively which personal data have been entered or modified in automated processing systems, at what time and by whom.

Measure	**A**
Logging of logon processes: Logging of the logon processes on the logon processes to the system	☒
Logging of failed access attempts: A corresponding logging is made	☒
Automated evaluation of log data: • Security measured • Audit log data will be audited for plausibility in the future	☒
Logging of deletion operations: • Audit log logs ist own deletion operations, • Data of the data subject is deleted immediately after the certificate is created, as can be seen from the source code.	☐

I. Transport control

Ensuring that the confidentiality and integrity of personal data is protected during the transmission of personal data as well as during the transport of data carriers.

Measure	**A**
Transport-encrypted data transmission: Data packets are always encrypted.	☒
Email encryption/transport encryption	☒
Documentation of the recipients of data and the time periods of the planned transfer or agreed deletion periods	☒

In physical transport: careful selection of transport personnel.	☒
Disclosure of data in anonymized or pseudonymized form	☒
Create an overview of regular retrieval and transmission operations	☒
During physical transport: secure transport containers/packaging	☒
Use of OSCI/XTA	☒
Web services (WS)-Security	☒

J. Data integrity

Ensuring that stored personal data cannot be damaged by system malfunctions.

Measure	**A**
Application of checksum methods: SHA-512 hash calculated from user data is signed.	☒
Malfunction of the apps during the generation of check results: The certificate generation code and verification algorithms are extensively tested before going live.	☒
Regular data backups and restore tests	☒
Self-repairing file systems are used	☒
Exclusive use of branded products of the highest (professional) quality for hardware	☒
Regular use of scrubbing, re-indexing, vacuuming, etc functionalities if available	☒
Journaling file systems are in use	☒

III. Availability and resilience (Art. 32 para. 1 lit. c GDPR) Ability to rapidly recover systems after a failure.

K. Recoverability

Deployed systems must be recoverable in the event of a failure.

Measure	**A**
Orchestration software is used (YADT, Ansible, Chef, Salt or Puppet)	☐
Regular data backups on SAN systems and tapes	☐
Virtualization wherever possible, so that virtual machines are recoverable on different hardware	☒
Emergency restart plans	☒
Virtual machine images are backed up/snapshots are created on a regular basis.	☒
Backup data center available	☒
Regular emergency drills	☒

L. Reliability

All functions of the system must be available and any malfunctions that occur must be reported.

Measure	**A**
A password policy to prevent simple passwords in the backend has been implemented and is technically monitored. The administrators of the relevant services are checked for reliability.	☒
Redundant Internet connection	☒
Denial of service attacks on the host servers resulting in intentional overload are mitigated by the following measures: ● All accesses to the host servers are designed redundantly and protected against a DoS attack by appropriate measures.	☒
Hardware/software support from manufacturer; usually highest possible availability level	☒
Malware scanner	☒
Phone hotline	☒
Ticket system with escalation function	☒
Server monitoring	☒
Alternate data center	☒
Regular emergency drills	☒
Notification via defined mailing lists in case of malfunction	☒
Ticket self-service system	☒
USV	☒
SMS notification in case of power failure	☒

M. Availability control

Personal data must be protected against destruction or loss.

Measure	**A**
Tiered data protection concept (incremental, full backups, snapshots, images)	☒
Storage of data backups in different fire zones: Backups are stored geo-redundantly in different data centers.	☒
Regular test of data recovery: Regular tests are performed and logged	☒
Contingency plan for restarting servers and services: A contingency plan exists.	☒
Automatic notification system in case of failure: An automatic notification is sent to the administrator in case of a system failure.	☒
Redundant IT systems: Data is processed geo-redundantly in different data centers.	☒

Virtualized infrastructure: A virtual infrastructure is used	☒
Load balancing: Load balancing implemented for network components, servers, and services. Automatic scaling of virtual systems.	☒
Fire extinguisher	☒

N. Separation Control

It must be possible to process personal data collected for different purposes separately (can be used optionally depending on the specialist procedure).

Measure	**A**
Separation of productive, staging, test and development system: Productive, staging, Test and Development system, are logically and physically separated from each other. Production data may only be used on the production environment (and also on staging if necessary).	☒
Client separation: A logical client separation exists. The implementation of client separation is checked as part of a code review.	☒

IV. Procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures (Art. 32 para. 1 lit. d GDPR)

O. Order control

Measure	**A**
Data secrecy: obligation of the contractor's employees to maintain data secrecy	☒
Data protection officer: The Contractor has appointed a data protection officer	☒
Control rights: Effective control rights vis-à-vis the contractor are agreed upon	☒
Documentation on existing IT infrastructure: Corresponding documentation is available	☒
Documentation on programs and applications used: ● Code libraries used are documented in the source code ● Directory of processing activities is available	☒
Verification of security measures: Examination of and documentation of the security measures taken at the contractor takes place in advance.	☒
Deletion of data: Data will be deleted after completion of the order in accordance with applicable retention periods.	☒
Written instructions to the contractor (by order data processing contract) according to Art. 28 para. 3 GDPR)	☐
Ongoing review of the contractor and its activities	☒

Ubirch operates a DSMS that is monitored by the data protection officer. A process for dealing with data breaches has been implemented.

Contact details of the data protection officer(s) (see sec. 4 para. 2 of the Agreement):

Gregor Klar
datenschutz@ubirch.com

established on 22nd of May 2024 (Ubirch/MJ)