Data Processing Agreement (DPA)
according to Article 28 – General Data Protection Regulation (GDPR)

between

represented by

– Controller –

hereinafter referred to as **“controller“**

and

Cryptshare AG

Schwarzwaldstr. 151

79102 Freiburg

represented by **Herr Oliver Kenk (CFO)**

– Processor –

hereinafter referred to as **“processor“**

jointly hereafter also specified as

contracting parties.

Table of Contents:

Preamble

There is an actual and legal cooperation between the controller and the processor in relation to services in the IT sector ("main contract"). Since it cannot be completely ruled out that the processor may gain or have access to client-specific personal data within the scope of implementation of this main contract, an agreement on the collection, processing and/ or use of personal data on behalf of the controller is required.

The processor shall handle personal data exclusively within the framework of the concluded agreements and in accordance to the instructions of the contracting authority, unless it is obliged to do so by law from the European Union or another Member State to which the processor is subject to (e.g. investigations by law enforcement or federal protection authorities). In such cases, the processor informs the controller of these legal requirements prior to processing, provided that the applicable law does not prohibit such a notification based on an important public interest (Art. 28 (3) p. 2 lit. a GDPR).

1 Subject-matter and agreement duration

1.1. Subject matter (Art. 28 (3) p. 1 GDPR)

☐ The subject matter of the agreement is specified in the attached service agreement which is being referred to here (hereinafter referred to as the service agreement).

or

☒ The subject matter of the agreement regarding data handling pertains to the execution of the following tasks by the processor:

- ✓ Support during software installation/configuration
- ✓ Providing manufacturer support, mainly by remote support, telephone or E-Mail during the term of the main contract
- ✓ Additional only, if demo access is used: Encryption, transmission and storage of electronic data through Cryptshare, according to the product description

1.2. Contract duration (Art. 28 (3) p. 1 GDPR)

☒ The duration of this agreement (term) corresponds to the term of the main contract

or

☐ The order is placed for one-time processing.

or

☐ The duration of this agreement (term) is limited until .....

or

☐ The agreement has been placed for an unlimited period and can be terminated by both parties with a notification period of..... on ..... . The possibility of termination without notice remain unaffected.

2 Data processing agreement specification

2.1. Nature and purpose of the intended data processing agreement (Art. 28 (3) p. 1 GDPR)

☒ The nature and purpose of processing personal data by the processor for the controller is specified in the main contract.

☐ The nature and purpose of processing personal data by the processor for the controller is specified in the attached service agreement.

or

☐ A detailed description of the contractual subject matter with regards to the nature and purpose of the processor's services: ....

The processing of data as contractually agreed shall take place exclusively in a European Union member state or in another contracting state belonging to the agreement on the European economic area.

2.2. Types of data

☐ The type of personal data used is defined in the attached service agreement.

or

☒ The subject matter of processing personal data pertains to the following data types/categories (list/ description of data categories)

- ☒ Personal identifiable data
- ☒ Communication data (e.g. telephone, e-mail, IP address)
- ☒ Contract reference data (contractual relationship, product or contractual interest)
- ☒ Customer history
- ☐ Contract billing and payment data
- ☐ Planning and operating data
- ☐ Disclosed information (from third parties, e.g. credit agencies, or from public directories)
- ☒ Within the scope of on-site or remote manufacturer support, insight and thereby processing of any conceivable form of personal data can arise for a short period of time, which is determined by customer behaviour.

2.3. Categories of affected persons

☐ A detailed category description of the data subjects affected by data processing are in the attached service agreement.

or

☒ The categories of data subjects covered by the data processing shall include:

- ☐ (Company name) customers
- ☒ Interested parties
- ☐ Subscribers
- ☐ Employees
- ☐ Suppliers
- ☐ Sales representative
- ☒ Contact
- ☐ Employees
- ☒ Within the scope of on-site or remote manufacturer support, insight and thereby processing of any conceivable form of personal data can arise for a short period of time, which is determined by customer behaviour.
- ☐ ...

3 Technical-organizational measures

3.1 The processor shall document the implementation of the technical and organizational measures and is required to provide them to the processor for inspection before contract begin and prior to the start of processing, especially with regards to the specific execution of contract. The documented measures become the basis of the agreement, after accepted by the controller. If the inspection/ audit of the client reveals a need for adjustment, this must be implemented by a mutual agreement.

3.2 The processor shall provide security in accordance with Art. 28 (3) lit. c, 32 GDPR, especially in connection with Art. 5 (1), (2) GDPR. Overall, the measures to be taken are data security measures and are to ensure a level of protection adequate to the risk regarding confidentiality, integrity, availability and reliability of the systems. The state of technology, implementation costs and the processing type, scope and purpose as well as the varying probability of risk, including the degree of risk to the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR must be considered. The details are specified in **Annex 1**.

3.3 The technical and organisational measures are subject to technical advancement and development. In this respect, the processor is entitled to implement alternative, adequate measures. The safety requirements of the defined measures must not be compromised. Significant changes must be documented.

4 Amendments, restrictions and data erasure

4.1 The processor may not correct, delete or restrict processing of the data that is being handled within the scope of the order on its own authority. This can only be performed after written consent of the controller. If an affected person contacts the processor regarding this matter in a direct fashion, the processor will immediately forward this request to the controller.

4.2 If included in the scope of services; the data erasure policy, the right to be forgotten, amendments, data portability and providing information according to written orders by the controller must be secured by the processor.

5 Quality assurance and other processor obligations

In addition to complying with the provisions of this agreement, the processor shall have legal obligations in accordance with Articles 28 to 33 GDPR. They must especially ensure compliance with the following regulations:

5.1 Written appointment of a data protection officer who performs his duties in accordance with Articles 38 and 39 of the GDPR.

a. The client's contact details are made available to the client via the company's homepage to make direct contact. A data protection officer change will be announced on the homepage.
b. The current contact details are easily accessible on the processor's homepage under the following link: https://www.cryptshare.com/en/privacy-and-cookie-policy/

5.2 Maintaining confidentiality according to Art. 28 (3) p. 2 lit. b, 29, 32 (4) GDPR. The processor only appoints employees who are bound to confidentiality and who have been previously familiarized with the data protection regulations relevant to them to conduct the work. The processor and any person subordinated to the processor who has access to personal identifiable data may process such data exclusively in accordance with the instructions of the controller, including the authorisation granted in this agreement, unless they are legally obliged to process such data.

5.3 The realisation and compliance with all technical and organisational measures required by this agreement in accordance with Art. 28 (3) sent. 2 lit. c, 32 GDPR. Details are specified in **Annex 1**.

5.4 Upon request, the controlling and processing parties shall mutually cooperate with regulatory authorities in the fulfilment of their obligations.

5.5 Providing the regulatory authorities with timely information regarding monitoring measures and actions taken as far as they relate to this agreement. This also applies to the case that a regulatory authority is conducting a criminal or disciplinary proceeding in relation to the processing of personal identifiable data during order processing for the controller.

5.6 If the controller is involved in an inspection by the regulatory authority, criminal or disciplinary proceedings, a liability claim of a third party or any other claim in connection with data processing within the scope of this agreement with the processor, the processor must provide support to the best of its' abilities.

5.7 The processor regularly monitors internal operations as well as technical and organisational measures to ensure that processing within its area of responsibility is being carried out in accordance with the regulations in force. This pertains to current data protection policies and the rights of the data subjects.

5.8 Evidence of the technical and organisational measures taken with respect to the controller within the scope of their authorized power in accordance with section 7 of this agreement.

6 Subcontracting

6.1 Sub-contracting relationships within the context of this agreement are defined as services which relate directly to supply the main service. This does not include supplementary services which the processor uses e.g. as telecommunication services, post/ transport services, maintenance and user services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and reliability of the hard- or software of data processing systems. However, the processor is required to take appropriate, legally-binding and monitoring measures to guarantee data protection and data security of the client's data, even in the case of outsourced subcontractual services.

6.2 The processor may only engage subcontractors (other processors) after prior written or documented client consent.

☐ Appointing a subcontractor is not permitted.

☒ The Controller agrees to the assignment of the following subcontractors subject to a contractual agreement in accordance with Art. 28 (2-4) GDPR:

No.	Subcontractor (Company name, Address)	Country	Service
1	Equinoxe GmbH Bismarckallee 9 79098 Freiburg i.Brg.	Germany	Additional only, if demo access is used: Hosting partner for Cryptshare demoserver
2	TeamViewer GmbH	Germany	Remote maintenance tool to access desktop device from contractees

☒ The addition of new subcontractors or replacement of existing subcontractors is permissible, if:

- the processor notifies the controller of such outsourcing to subcontractors in written form in a reasonable time in advance and
- the controller does not object to the planned outsourcing in written form and/ or due to a compelling reason towards the processor within 14 days after notification and
- a contractual agreement in accordance with Art. 28 (2-4) GDPR is taken as a reference.

6.3 The first-time transfer of the client's personal data to the subcontractor is only permitted if all requirements for a company contract are met.

6.4 If the subcontractor performs the agreed service outside the EU/EEA, the processor must take appropriate measures to ensure data protection admissibility. The same applies if service providers are used within the scope of paragraph 1, sentence 2.

6.5 Further outsourcing by the subcontractor

☐ is not allowed;
☐ requires written consent from the main controller (must be in text form);
☒ requires written consent from the main processor (must be in text form);

6.6 All contractual agreements in the contract chain must also be imposed on the other subcontractors.

7 Controller obligations

7.1 The controller has the right to carry out inspections in consultation with the processor or to have them carried out by appointed auditors. He has the right to verify the processor's compliance with this agreement within their business operations by means of sample audits, which must be notified in advance.

7.2 The processor shall ensure that the controller can verify compliance with controller obligations in accordance with Art. 28 GDPR. The processor is obliged to provide the controller with the necessary information upon request and especially to prove the implementation of the technical and organisational measures.

7.3 The processor may assert a claim for compensation in order to enable controller-originated inspections.

8 Processor contract breach notification

8.1 The processor shall assist the controlling entity in complying with the obligations set out in Articles 32 to 36 of the GDPR concerning the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes:

a. the assurance of an adequate level of protection by technical and organisational measures which take the circumstances and purposes of data processing into account, as well as the predicted risk and severity of possible legal violations due to security vulnerabilities and make an immediate determination of relevant violations possible.
b. the obligation to report such violations of personal data to the controller without delay
c. the obligation to support the controller in the context of his duty to inform the affected person and to immediately make all relevant information available to them in connection hereto.
d. to support the controller in their data protection impact assessment
e. to support the client in prior consultations with the regulatory authorities.

8.2 The processor may claim remuneration for support services which are not included in the service description or are not attributable to processor misconduct.

9 Controller's authority to issue directives

9.1 The client confirms verbal instructions without delay (must be in text form).

9.2 The processor must inform the controller immediately if they think that a directive violates data protection regulations. The processor is entitled to postpone order fulfilment of the corresponding instruction until it is confirmed or changed by the controller.

10 Erasure and return of personal data

10.1 Copies or duplicates of the data will not be made without the controller's knowledge. This excludes backup copies, if they are necessary to guarantee proper data processing, as well as data for which it is necessary to store in order to comply with legal storage obligations.

10.2 After completion of the contractually agreed work, or earlier, upon request by the controller - or upon termination of the service agreement at the latest; the processor must hand over all documents that were produced within the scope of the data processing agreement. These data sets that were created in connection with the contractual relationship, must be handed back to the controller or, with prior consent, destroyed in accordance with data protection regulations. The same applies to test and discarded material. The erasure protocol must be submitted upon request.

10.3 Documentation that serves as proof of proper order and data processing must be kept by the processor after the end of the contract in accordance with the respective retention periods. They can hand them over to the controller at the end of the contract.

Controller	**Processor**
	Cryptshare AG
_____	_____
Name (in capital letters)	Name (in capital letters)
	Oliver Kenk (CFO)
_____	_____
Role / Title	Role / Title
	Freiburg,
_____	_____
Place, Date	Place, Date
_____	_____
Signature	Signature

Annex 1 (Technical-organizational measures according to GDPR)

Supplement to the Data Processing Agreement

from

and Cryptshare AG on

1. Confidentiality (Art. 32 (1) lit. B GDPR)

- ✓ Access control
    - The offices are locked during and after business hours and can only be entered by authorised personnel.
    - The offices are alarm-secured during non-business hours.
    - All exterior doors can only be opened with a special key.
    - The server area is locked separately, is alarm-protected and can only be entered by a limited number of people.
    - Authorized employees receive access to the server area, after receiving a key and a token upon signing an additional agreement as well as a confidentiality agreement.
- ✓ Access control
    - Use of data encryption
    - User identification and password procedures
    - Use of a hardware firewall
    - Use of anti-virus software
    - Use of VPN technology for remote access
    - Use of Mobile Device Management
    - Administration of user authorizations
    - Careful selection of employees that includes the cleaning staff as well
- ✓ Access control
    - Use of document shredders
    - Access logs to applications, especially when entering, modifying and erasing data.
    - Authorization concept and access rights, adapted to responsibility areas and according to the need-to-know principle
    - Password policy
    - Administration of user rights by system administrators
    - The number of administrators of the system is limited to the very essentials.

- ✓ Separation control
    - Production and test systems are separated from one another.
    - There is no personal data of the controller on development and test systems
    - Application of an authorization concept with different access rights
    - The storage of personal and non-personal data is conducted in separate databases with different access rights

2. Integrity (Art. 32 (1) lit. B GDPR)

- ✓ Transfer control
    - Use of VPN tunnels for remote access to data by employees
    - Use of e-mail encryption and encrypted file transfer for communication with customers
    - As part of the Cryptshare support, personal data will not be passed on to third parties.
- ✓ Input control
    - Logging of the entry, modification and erasure of data
    - Assignment of rights to enter, modify and erase data based on an authorization concept
    - Overview creation of which applications are being used to enter, modify and erase which data.

3. Availability and reliability (Art. 32 (1) lit. B GDPR)

- ✓ Availability check
    - The server room is located in the building above the flood line
    - The server room is not below sanitary facilities
    - Fire extinguishers are located in the server room
    - A physical data backup system exists
    - Two server systems are operated parallel to each other

- ✓ Rapid recoverability
    - Eine Wiederherstellung bei Datenverlust kann auf Basis der vorhandenen Sicherungseinrichtungen innerhalb von ca. 24 Stunden erfolgen.

4. Procedures for routine review, assessment and evaluation (Art. 32 (1) lit. D GDPR; Art. 25 (1) GDPR)

- ✓ Data Protection Management
    - The contractor is in possession of the legally mandatory data protection management.
- ✓ Incident-response management
    - The most current codes of conduct related to data protection are available on the processor's intranet and are accessible to all employees.
- ✓ Data protection-friendly default settings (Art. 25 (2) GDPR)
    - The company has authorization and access concepts in place to ensure personal data accessibility.
- ✓ Order control
    - Subcontractors are carefully selected with special consideration to legal regulations of "collection, processing or personal data use on behalf of" and thus the qualification of technical and organizational measures taken by them.
    - The collection, processing and erasure of the data is strictly bound to the agreement and client-specific instructions in accordance with the agreements laid down in the data processing agreement.

5. Anonymisation (Art. 32 (1) lit. B GDPR)

- ✓ Personal data collected or generated within the scope of support activities or are anonymised by applicable technical measures.
- ✓ The anonymisation takes place on a regular basis shortly after completion of the support activities.