Annex C – Data Privacy and Agreement on the processing of personal data

Current as of: August 30, 2021

Disclaimer:

The following translation of the MOXIS Cloud Service Terms into the English language has been made with great care, yet it is merely a service for your convenience and has no legal binding force. Upon conclusion of a contract, only the original German version of the MOXIS Cloud Service Terms is binding, which you can access at: https://www.xitrust.com/agb/

Contents

1. Scope

This annex C is part of the MOXIS Cloud Service Terms (including all annexes and documents referred to) govern the contractual relationship between the Customer and XiTrust Secure Technologies GmbH, FN 219152h, headquartered in A-8010 Graz, Grazbachgasse 67, referred to below as "XiTrust", for the use of the "MOXIS" software as MOXIS Cloud Service (as defined below).

Annex C - Agreement on the processing of personal data for MOXIS Cloud Services in accordance with Art. 28 GDPR ("DPA") - applicable to Customers and Affiliates in the EU

1. Background

This DPA applies to Personal Data processed by XiTrust in connection with the provision of the MOXIS Cloud Service as a processor.

The Customer, affiliates and business partners act as data controllers within the meaning of the GDPR and are responsible for the legal conformity of the processing of Personal Data in accordance with this DPA.

To the extent that authorizations, approvals, instructions or permissions are issued by the Customer, these are issued not only in the name of the Customer but also in the name of the additional persons responsible. When XiTrust informs or sends notices to the Customer, such information or notices shall be deemed to have been received from the responsible parties whom the Customer has authorized to use the MOXIS Cloud Service. It is the Customer's responsibility to forward this information and these notices to the appropriate responsible parties.

Attachments 1 and 2 are an integral part of this DPA. Annex 1 sets out the agreed subject matter, the nature and purpose of the processing, the type of Personal Data, the categories of Data Subjects and Annex 2 sets out the Technical and Organizational Measures to be applied.

2. Definitions

Data protection rules: encompassing the GDPR and the Data Protection Act (DSG)

GDPR: refers to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (the General Data Protection Regulation).

DSG: Federal Law on the Protection of Individuals with regard to the Processing of Personal Data (Data Protection Act - DSG)

Personal Data: refers to any information relating to a Data Subject, and in this DPA only refers to Personal Data that is (i) collected by or through the use of Authorized Users in the MOXIS Cloud Service, or (ii) provided or accessed by XiTrust and its sub-processors in order to provide the Services. Personal Data is a subset of Customer Data (see the definition in the body of the MOXIS Cloud Service Terms).

Sub-processor: refers to other processors who are commissioned by XiTrust to carry out the processing

For terms used in this DPA or in Annexes 1 and 2, but not defined in this DPA or in the main part of the MOXIS Cloud Provisions, the definitions according to the GDPR shall apply.

3. Notices from XiTrust to the Customer; initiating contact with XiTrust

Notices from XiTrust to the Customer within the scope of this DPA, in particular also notices of violations of the protection of personal data, are sent via e-mail to the contact person designated by the Customer.

The Customer is obligated to ensure that XiTrust always has the current contact information of the Customer's contact person.

If the Customer believes that XiTrust is not fulfilling its data protection and security obligations, the Customer may contact XiTrust's Data Protection Coordinator at the e-mail address datenschutz@xitrust.com (Note: XiTrust is not required to appoint a Data Protection Officer).

4. Security of data processing

4.1 Appropriate Technical and Organizational Measures

XiTrust has implemented the Technical and Organizational Measures ("TOMs") specified in Attachment 2. Customer has reviewed these TOMs and agrees that these TOMs are appropriate with respect to the MOXIS Cloud Service, taking into account the state of the art, implementation costs, nature, scope, context and purpose of the processing of personal data.

4.2 Changes

XiTrust applies the TOMs described in Attachment 2 equally to all customers hosted in the same data center and receiving the same MOXIS Cloud Service. XiTrust may change the measures listed in Attachment 2 at any time without notice as long as it maintains a comparable or better level of security.

4.3 Data protection devices

The Customer is responsible for implementing and maintaining data protection devices and security measures for components that the Customer provides or controls.

5. Duties of XiTrust

5.1 Instructions of the Customer as the Controller

XiTrust will process personal data only in accordance with the documented instructions of the Customer. This DPA constitutes such a documented instruction, and any use of the MOXIS Cloud Service by Customer shall then constitute further instructions.

XiTrust will inform the Customer immediately if it believes that an instruction violates data protection regulations. XiTrust is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the Customer.

5.2 Quality Assurance

XiTrust and its sub-processors only use authorized persons for the processing of personal data who have been obligated to maintain confidentiality and have been familiarized with the relevant data protection regulations beforehand. XiTrust and any persons engaged by XiTrust and its sub-processors who have access to Personal Data may process such data solely in accordance with the Customer's instructions, including the powers granted in this Agreement, unless they are required by law to process it.

5.3 Support of the Customer

The Customer is solely responsible for complying with its obligations as a responsible party, including its reporting obligations.

XiTrust shall adequately support the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of the processing of Personal Data, reporting Personal Data breaches to the supervisory authority, notification of the person affected by a Personal Data breach, data protection impact assessment and prior consultation.

Upon the Customer's request, XiTrust will reasonably cooperate with the Customer to address inquiries from Data Subjects or supervisory authorities regarding XiTrust's processing of Personal Data or Personal Data breaches.

If a Data Subject directly contacts XiTrust regarding the processing of customer data, XiTrust will immediately forward this request to the Customer without responding to this request itself, without further instructions from the Customer.

5.4 Personal data breach notifications

XiTrust will immediately notify the Customer of a Personal Data breach after becoming aware of it and will provide the Customer with appropriate information available to XiTrust to assist the Customer in fulfilling its obligations to report a Personal Data breach in accordance with the requirements of data protection law.

6. Data export and deletion

At any time during the term of the Agreement, the Customer shall have the option to access, extract, correct and erase the Personal Data stored in the MOXIS Cloud Service. However, in this context XiTrust expressly refers to the Customer's obligation to the data security measures according to Section 8.5 of the main part of the MOXIS Cloud Service Terms.

At the end of the term, the Customer is no longer entitled to use the MOXIS Cloud Service and XiTrust's confidential information. For 30 calendar days after the end of the term, XiTrust will only grant the Customer and Affiliates access to the MOXIS Cloud Service for the sole purpose of backing up the data so that the Customer can finally extract the data (this is equivalent to returning the Personal Data).

The MOXIS Cloud Service may not support the software that the Customer provides for extraction. XiTrust assumes no liability for the extraction of customer data.

The Customer hereby instructs XiTrust to completely erase all remaining customer data created in connection with the provision of the MOXIS Cloud Service after the end of the contract, unless XiTrust is required to retain such data under applicable law.

7. Control rights of the Customer as Controller

XiTrust will regularly check compliance with the obligations agreed upon in this DPA and prepare audit reports. XiTrust will make these audit reports available to the Customer upon request. Test reports are confidential information and are subject to the confidentiality agreement of the MOXIS Cloud Service Terms.

To the extent that Customer's control requirements cannot be adequately met by providing the audit reports and other information requested by Customer for this purpose, Customer or an auditor appointed by Customer may audit the control environment and compliance with the Technical and Organizational Measures (TOMs) protecting the MOXIS Cloud Service production systems at its own expense, subject to mutually agreed scheduling, unless the audit is formally conducted by a regulatory authority. XiTrust may object to the selection of the assigned auditor in the event of factual objections based on the person of the appointed auditor. The Customer will not be granted access to the data of other customers of XiTrust or facilities or systems that are not related to the provision of the MOXIS Cloud Service.

8. Sub-processors

8.1 Permitted use

The Customer hereby grants XiTrust its prior general written consent to transfer the processing of Personal Data to sub-processors under the following conditions:

- ✓ XiTrust engages sub-processors on the basis of written contracts in accordance with Art 28 GDPR, which comply with the provisions of these DPA with respect to the processing of Personal Data by the sub-processor, in particular the appropriate technical and organizational measures. XiTrust shall be liable for any violations by the subcontracted processor in accordance with the MOXIS Cloud Service Terms.
- ✓ The list of XiTrust's sub-processors valid at the time the contract is concluded, including their scope of activities, will be made available to the Customer upon request.

8.2 New Sub-processors

The use of new sub-processors is at the discretion of XiTrust under the following conditions:

- ✓ XiTrust shall inform the Customer as the Controller party in advance by e-mail about the planned additions or replacements within the list of sub-processors and their areas of activity.
- ✓ The Customer as the Controller shall be given the opportunity to object to such changes in accordance with Section 8.3.

8.3 Objection to new sub-processors

If the Customer has a legitimate reason under data protection law to object to the processing of Personal Data by the new sub-processor(s) for the provision of MOXIS Cloud Service under the Agreement, the Customer may terminate the Agreement by giving written notice to XiTrust, Attn: Data Protection Coordinator, within 30 days from the date of XiTrust's notice of the new Sub-Processor, effective on a date specified by the Customer. If the Customer does not terminate the contract within the 30-day period, the new sub-processor shall be deemed to have been approved by the Customer.

Any termination under this provision shall be deemed by the parties to be without fault.

8.4 Emergency Exchange

XiTrust may replace a sub-processor without prior notice if the immediate replacement is necessary for security or other reasons. In this case, XiTrust shall inform the Customer about the new sub-processor immediately after its appointment. Section 8.3 applies mutatis mutandis.

9. Documentation; processing directory

Each party is responsible for complying with its documentation obligations under data protection law, in particular for maintaining procedure directories. Each Party shall provide reasonable assistance to the other Party in fulfilling its documentation obligations.

Attachment 1 to Annex C – Subject, purpose and duration of the processing of personal data

Object and purpose

XiTrust processes customer data as part of the DPA exclusively in connection with the provision of the MOXIS Cloud Service for the Customer and its affiliates necessary for the use and rendering of software support and software maintenance. Personal data is processed in connection to the following:

- ✓ Processing of personal data to configure, operate and provide the MOXIS Cloud Service.
- ✓ Communication with authorized users (exclusively to provide software maintenance and software support services).
- ✓ Storing personal data in data centers of sub-processors.
- ✓ Upload for correction purposes, service packs, updates or upgrades in the MOXIS Cloud Service.
- ✓ Creation of backups of persona data.
- ✓ Network access to enable the transfer of personal data.
- ✓ Execution of instructions of the Customer according to the Agreement.

Duration of the personal data processing

The term of the DPA corresponds to the contract term between the Customer and XiTrust in connection to the MOXIS Cloud Service.

Location of the processing of personal data

The processing of Personal Data takes place exclusively within the EU.

Data subjects

Data subjects can generally be classified as follows: Data subjects can generally be classified as follows: authorized users, such as employees, business partners or other persons, whose personal data is stored in the MOXIS Cloud Service.

Data categories:

In general, personal data can be classified as follows: In general, personal data can be classified as follows: contact data (e.g., name, address, telephone, email), system access/use/credentials, name of the company, contract data, invoice data and data subject to specific applications, which are collected by authorized users of the Customers in the MOXIS Cloud Service..

Special data categories (if given)

The personal data may also be classified in the special data categories set out in the contract.

Attachment 2 to Annex C – Technical and Organizational Measures

XiTrust and its subcontractors have taken the following technical and organizational measures for the use of the MOXIS Cloud Service:

Confidentiality (Art. 32 para 1 lit b GDPR)	
Physical access control As part of the physical **access control** unauthorized persons shall not be allowed to physically enter the data processing facilities, where personal data are processed. Unauthorized persons shall be prevented from getting closer to the unattended data processing facilities. This way the possibility that an unauthorized party might gain knowledge or influence will be excluded from the beginning.	XiTrust: • Security locks • Access not possible from outside • Alarm system • Visitors monitoring • Process to revoke credentials that are no longer needed
	Data center • Magnet or chip cards • Electric door opener • Security staff • Concierge • Alarm and video system
Data access control The unauthorized use of data processing systems will be hindered through **data access control**. The perpetration into the system is protected even for unauthorized persons outside the system.	XiTrust: • (Secure) passwords (including the corresponding policy) • User authentication • Automatic locking mechanism • Separating company and guest Wi-Fi • Security actions for external access to the company's network e.g., work from home (virtual private network) • Guideline on secure use of mobile devices • No use of private terminal devices • Encryption of data media
	Data center • (Secure) passwords (including the corresponding policy) • Automatic locking mechanism • Two factor authentication • Encryption of data media
Access authorization control **Access authorization control** ensures that the persons authorized to use a data processing system exclusively have access to the data that correspond to their access authorization and that personal data during the processing, use and after being stored cannot be read, copied, changed or deleted without authorization. This way access and storage measures are both controlled. In terms of organizational matters, the access control ensures that the access is only granted for data required by the employee to accomplish the tasks They have been assigned to.	XiTrust: • Standard authorization profiles on a 'need-to-know' basis • Standard process to grant access • Access log • Regular testing of the authorizations granted, especially for administrative user accounts • Process to revoke credentials that are no longer needed
	Data center • Standard authorization profiles on a 'need-to-know' basis • Standard process to grant access • Access log

	- Regular testing of the authorizations granted, especially for administrative user accounts
Separation control As part of the separation rule, XiTrust ensures that data collected for different purposes will be processed separately.	XiTrust: - Client separation - Separation of productive and test system (Private Cloud) - Physically separated storage on separated systems (Private Cloud)
	Data center - Multi-client capability - Sandboxing
Pseudonymization The processing of personal data is carried out in such a manner that it cannot longer be attributed to a specific data subject without additional information, provided that such additional information is stored separately and is subject to technical and organizational measures.	XiTrust: - Provider shielding - No targeted reading of personal data in documents
	Data center If necessary or appropriate for the respective data processing, the primary identifiers of the Personal Data in the respective data application shall be removed so that the data can no longer be attributed to a specific data subject without the use of additional information, and such additional information shall be kept separately and shall be subject to appropriate technical and organizational measures
Integrity (Art. 32 para 1 lit b GDPR)	
Transfer control **Transfer control** prevents data carriers from being read, copied, removed or modified without authorization and to verify when data transmission is taking place.	XiTrust: - No unauthorized reading, copying, modifying or removing during data transfer or transport. - Encryption - Virtual private networks - Protected connection from and to the data center - No data transfer during the singing process /Hash value procedure)
	Data center - No unauthorized reading, copying, modifying or removing during data transfer or transport. - Encryption - Virtual private networks
Entry control **Entry control** ensures that it can be traced back when and by whom personal data has been entered, changed, deleted or removed in the data processing system.	XiTrust: - Logging of whether or by whom personal data has been entered, changed or removed in the data processing system - Entering, modifying or removing data is only possible in cooperation with the data controller.
	Data center - Logging of whether or by whom personal data has been entered, changed or removed in the data processing system
Availability and resilience (Art. 32 para 1 lit b GDPR)	

Availability control By means of these measures it is ensured that data is protected from accidental destruction or loss and always available for the Customer or ordering party.	XiTrust: • Backup strategy • Virus protection • Firewall • Standard processes when employees enter/leave the company
	Data center • Backup strategy (online/offline, on-site/off-site) • Uninterrupted power supply (USV diesel generator) • Virus protection • Firewall • Reporting channels and emergency plans • Security checks of the infrastructure and at application levels. • Multi-staged security concept and data encryption to alternative data centers. • Standard processes when employees enter/leave the company • Rapid recovery (Art. 32 para 1 lit c GDPR)
Process for regularly testing assessing and evaluating (Art. 32 para 1 lit b GDPR)	
Data protection management Following measures guarantee the existence of an organization that fulfils the basic statutory data protection requirements.	XiTrust: • Data protection management including continuous staff training • Incident-response processes • Order control: no order processing without the corresponding instructions and • An unambiguous contract • Formalized order management • Strict selection of the service provider • Vetting duty • Follow-up controls • Confidentiality obligation of the employees • Assignment of a data protection manager • Regular audit of the technical and organizational measures for data protection
	Data center • Data protection management including continuous staff training • Incident-response processes • Order control: no order processing without the corresponding instructions and • An unambiguous contract • Formalized order management • Strict selection of the service provider • Vetting duty • Follow-up controls
Data protection through technology design and data protection-friendly defaults (Art. 25 para 1 and 2 GDPR)	

Data protection through technology design Following measures guarantee the existence of an organization that fulfils the basic statutory data protection requirements.	MOXIS: • Option to validate the correctness of personal data • Personal data is stored only as long as it is required for the pursued purpose (automatic erasure concept). • Guarantee of integrity and confidentiality of personal data through technical measures and concepts, e.g. through authorization concept, traceability of changes, protection against manipulation, zone segmenting • Processes for data subject queries • Possibility of correction, deletion and restriction of the processing of personal data • Regular validation of the software by means of independent tools and penetration tests
Data protection-friendly defaults Following measures guarantee the existence of an organization that fulfils the basic statutory data protection requirements.	MOXIS is set up and configured in such a way that only personal data can be processed that is required for the relevant purpose being pursued.