Data processing agreement (DPA)

Document Classification:	Public
Version:	2.0
Date:	8 December 2025
Document Author:	Michael Seidl
Document Owner:	Information Security Officer

Data Processing Agreement (DPA)

between

XU Group GmbH,

Mehringdamm 33, 10961 Berlin,
registered in the commercial register of the Charlottenburg Local Court under HRB 172976 B,
represented by the managing directors Nicole Gaiziunas-Jahns and Dr Christopher Jahns,

– hereinafter referred to as "processor, contractor, provider or XU" –

and

Client

– hereinafter referred to as "controller, customer" –

– hereinafter also referred to as "Parties" –

SECTION I

Standard contractual clauses

Clause 1: Purpose and scope

a) The purpose of these standard contractual clauses ("Clauses") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b) The controllers and processors listed in Annex I have agreed to these clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

c) These clauses apply to the processing of personal data as set out in Annex II.

d) Annexes I to IV form an integral part of the clauses.

e) These clauses apply without prejudice to the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These clauses do not in themselves guarantee that the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 are fulfilled.

Clause 2: Immutability of the clauses

The parties agree to incorporate the European Commission's standard contractual clauses for the relationship between controllers and processors pursuant to Art. 28(7) and (8) GDPR (Commission Decision of 4 June 2021) into this data processing agreement. The parties undertake not to amend the core text of these standard contractual clauses. Only the information provided in the annexes may be supplemented and updated. The parties may incorporate the standard contractual clauses into a more comprehensive contract and agree on additional clauses or guarantees, provided that these do not directly or indirectly contradict the standard contractual clauses and do not affect the fundamental rights or freedoms of the data subjects. In the event of a conflict between these standard contractual clauses and other provisions of this contract or related agreements, the standard contractual clauses shall prevail.

Clause 3: Interpretation

a) Where terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 are used in these clauses, those terms shall have the same meaning as in the respective Regulation.

b) These clauses shall be interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

c) These clauses shall not be interpreted in a manner that conflicts with the rights and obligations provided for in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 or that restricts the fundamental rights or freedoms of the data subjects.

Clause 4: Precedence

In the event of any conflict between these clauses and the provisions of existing or subsequent agreements between the parties, these clauses shall prevail.

Clause 5: Tying clause

a) An organization that is not a party to these clauses may, with the consent of all parties, join these clauses at any time as a controller or processor by completing the appendices and signing Appendix I.

b) After completing and signing the appendices referred to in point (a), the acceding body shall be treated as a party to these clauses and shall have the rights and obligations of a controller or processor in accordance with Appendix I.

c) The rights and obligations under these clauses shall not apply to the acceding body for the period prior to its accession as a party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6: Description of the processing

The details of the processing operations, in particular the categories of personal data and the purposes for which the personal data are processed on behalf of the controller, are set out in Annex II.

Clause 7: Obligations of the Parties

1. Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of those legal requirements before processing, unless it is not permitted for reasons of public interest under the relevant law. The controller may issue further instructions throughout the entire period of processing of personal data. These instructions must always be documented.

b) Instructions from the controller shall be received via it@xu.de . Only designated persons are authorized to issue instructions. The processor shall document the instructions issued and their implementation.

c) The processor shall inform the controller without delay if it considers that the instructions of the controller are contrary to Regulation (EU) 2016/679, Regulation (EU) 2018/1725 or applicable data protection regulations of the Union or a Member State.

2. Purpose limitation

The processor shall process the personal data only for the specific purposes set out in Annex II, unless it receives further instructions from the controller.

3. Duration of processing of personal data

The data shall be processed by the processor only for the period specified in Annex II.

4. Security of processing

a) The processor shall implement at least the technical and organizational measures specified in the **technical and organizational measures** (TOM) to ensure the security of the personal data. This includes protecting the data against a security breach that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or access to the data (hereinafter referred to as a "personal data breach"). When assessing the appropriate level of protection, the parties shall consider the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to data subjects.

b) The processor shall grant its employees access to the personal data being processed only to the extent that is strictly necessary for the performance, management and monitoring of the contract. The processor shall ensure that the persons authorized to process the personal data received have committed themselves to confidentiality or are subject to a corresponding legal confidentiality obligation.

5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or data containing genetic data or biometric data for the unique identification of a natural person, data concerning health, sexual life or sexual orientation of a person, or data concerning criminal convictions and offences (hereinafter "sensitive data"), the processor shall apply special restrictions and/or additional safeguards.

6. Documentation and compliance with the clauses

a) The parties must be able to demonstrate compliance with these clauses.

b) The processor shall respond promptly and appropriately to requests from the controller regarding the processing of data under these clauses.

c) The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations laid down in these clauses and resulting directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the request of the controller, the processor shall also facilitate and contribute to the verification of the processing operations covered by these clauses at reasonable intervals or in the event of indications of non-compliance. When deciding on a verification or audit, the controller may consider relevant certifications of the processor.

d) The controller may conduct the audit itself or engage an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall be conducted after reasonable notice, where appropriate.

e) The parties shall provide the competent supervisory authority or authorities with the information referred to in this clause, including the results of the audits, upon request.

7. Use of sub-processors

a) The processor is generally authorized by the controller to engage sub-processors listed in an agreed list. The processor shall notify the controller in writing at least two weeks in advance of any intended changes to this list by adding or replacing sub-processors, so that the controller has sufficient time to object to such changes before the relevant sub-processor(s) are engaged.

The processor shall provide the controller with the information necessary to exercise its right to object.

b) If the processor engages a sub-processor to carry out specific processing operations (on behalf of the controller), this engagement must be by contract imposing on the sub-processor substantially the same data protection obligations as are imposed on the processor under these clauses. The processor shall ensure that the sub-processor fulfils the obligations to which the processor is subject under these clauses and under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall provide the controller with a copy of this sub-processing agreement and any subsequent amendments upon request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the processor may redact the text of the agreement before disclosing a copy.

d) The processor shall be fully liable to the controller for the compliance of the sub-processor with the obligations arising from the contract concluded with the processor. The processor shall notify the controller if the sub-processor fails to comply with its contractual obligations.

e) The processor shall conclude a third-party beneficiary clause with the sub-processor, according to which the controller shall have the right, in the event of the actual or legal termination of the processor or its insolvency, to terminate the sub-processing agreement and instruct the sub-processor to delete or return the personal data.

8. International data transfers

a) Any transfer of data by the processor to a third country or an international organization shall be carried out exclusively on the basis of documented instructions from the controller or in order to comply with a specific provision of Union law or the law of a Member State to which the processor is subject, and shall comply with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that in cases where the processor engages a sub-processor to carry out certain processing operations (on behalf of the controller) in accordance with clause 7.7 and these processing operations involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor shall ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for the application of these standard contractual clauses are met.

Clause 8: Assistance to the controller

a) The processor shall inform the controller without delay of any requests from the data subject. It shall not respond to the request itself unless authorized to do so by the controller. The processor shall notify the controller without delay of any legal requests for access from third parties, such as public authorities, to the extent permitted by law. It shall verify the lawfulness of the request, demand the evidence required by law, provide only the minimum necessary information and challenge any unlawful or excessive orders. Transparency reports shall be provided where permitted.

b) Considering the nature of the processing, the processor shall support the controller in fulfilling its obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under points (a) and (b), the processor shall follow the instructions of the controller.

c) In addition to its obligation under clause 8(b), the processor shall assist the controller, considering the nature of the data processing and the information available to it, the processor shall assist the controller in fulfilling the following obligations:
   - the obligation to carry out a data protection impact assessment on the planned processing operations (hereinafter referred to as "data protection impact assessment") if a form of processing is likely to result in a high risk to the rights and freedoms of natural persons.
   - the obligation to consult the competent supervisory authority or authorities prior to processing if a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk.
   - the obligation to ensure the accuracy of personal data by informing the controller without delay if it is found that the personal data processed by the controller is inaccurate or out of date.
   - Obligations under Article 32 of Regulation (EU) 2016/679.

d) The parties shall specify in the **technical and organizational measures** (TOM) the appropriate measures by which the processor shall assist the controller in applying this clause, as well as the scope and extent of the assistance required.

Clause 9: Notification of personal data breaches

In the event of a personal data breach, the processor shall cooperate with and assist the controller so that the latter can fulfil its obligations pursuant to Articles 33 and 34 of Regulation (EU) 2016/679 or, where applicable, Articles 34 and 35 of Regulation (EU) 2018/1725, taking into account the nature of the processing and the information available to it.

1. Breach of data protection during processing by the controller

The processor shall notify the controller of any personal data breaches without delay, at the latest within 24 hours of becoming aware of them, via the contact details provided by the controller. The initial notification shall contain at least the information specified in Article 33(3) GDPR (if available); any missing information shall be provided without delay. Notifications to supervisory authorities or data subjects shall be made exclusively by the controller or on the controller's documented instructions.

In the event of a personal data breach relating to the data processed by the controller, the processor shall support the controller as follows:

a) immediate notification of the personal data breach to the competent supervisory authority(ies) after the controller becomes aware of the breach, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).

b) when obtaining the following information, which must be included in the controller's report in accordance with Article 33(3) of Regulation (EU) 2016/679 and must include at least the following:

   - the nature of the personal data, where possible specifying the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned.
   - the likely consequences of the personal data breach.
   - the measures taken or proposed by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

   Where not all of this information can be provided at the same time, the initial notification shall contain the information available at that time, and further information shall be provided without delay as soon as it becomes available.

c) in accordance with the obligation laid down in Article 34 of Regulation (EU) 2016/679 to inform the data subject without delay of the personal data breach where that breach is likely to result in a high risk to the rights and freedoms of natural persons.

2. Breach of the protection of data processed by the processor

In the event of a personal data breach relating to data processed by the processor, the processor shall notify the controller without delay after becoming aware of the breach. This notification shall include at least the following information:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects concerned and the approximate number of data records concerned).

b) the contact details of a contact point from which further information about the personal data breach can be obtained.

c) the likely consequences and the measures already taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

If and to the extent that not all of this information can be provided at the same time, the initial notification shall contain the information available at that time, and further information shall be provided without delay as soon as it becomes available.

The parties shall specify in the **technical and organisational measures** (TOM) any further information that the processor must provide to assist the controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10: Breach of the clauses and termination of the agreement

a) Without prejudice to the provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the Processor fails to comply with its obligations under these Clauses, the Controller may instruct the Processor to suspend the processing of personal data until it complies with these Clauses or the contract is terminated. The processor shall inform the controller without delay if, for any reason, it is unable to comply with these clauses.

b) The controller shall have the right to terminate the contract insofar as it concerns the processing of personal data under these clauses if

- the controller has suspended the processing of personal data by the processor in accordance with point (a) and compliance with these clauses has not been restored within a reasonable period of time, and in any event within one month of the suspension.
- the processor has materially or repeatedly breached these clauses or failed to comply with its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- the processor fails to comply with a binding decision of a competent court or competent supervisory authority(ies) in relation to its obligations under these clauses, Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

d) The processor shall be entitled to terminate the contract insofar as it relates to the processing of personal data under these clauses if the controller insists on complying with its instructions after having been informed by the processor that its instructions violate applicable legal provisions in accordance with clause 7.1(b).

e) Upon termination of the contract, the processor shall, at the controller's discretion, delete all personal data processed on behalf of the controller and confirm to the controller that this has been done, or return all personal data to the controller and delete any existing copies, unless there is an obligation to retain data under Union or Member State law ( ). Until the data is deleted or returned, the processor shall continue to ensure compliance with these clauses.

ANNEX I

Processor:

Name:	*XU Group GmbH*
Address:	*Mehringdamm 33, 10961 Berlin*
Name, position and contact details:	*Michael Seidl,* *Head of Business Technology & Information Security*

Name:	*Projekt 29 GmbH & Co. KG*
Address:	*Ostengasse 14, 93047 Regensburg*
Name, position and contact details:	*Christian Volkmer, Data Protection Officer*

ANNEX II

Description of processing

Categories of data subjects whose personal data is processed

Users who register on the XU platform. These users are customers of the client.

Categories of personal data processed

In order to register for the XU platform, XU generally requires the following personal data:

- Email address
- Full name

XU uses three methods to register for the XU platform:

Direct invitations: We send potential users personalized email invitations with a registration link. As part of this process, first and last names are collected to personalize the invitation. Recipients must complete the registration process to gain access to the platform. Compliance with data protection laws is ensured by obtaining the necessary consents prior to the collection and use of personal data.

The selection of the legal basis (including any consents) and the fulfilment of the information obligations towards data subjects are the responsibility of the controller. The processor does not obtain consents on its own behalf unless this has been separately agreed in writing.

Self-registration: With this method, individuals can register directly on the platform without prior invitation, provided they have an email address from an approved domain. This ensures that registration is restricted to specific organizations or groups. There are no additional age or identity checks, which simplifies the onboarding process.

Token access: Tokens are distributed to eligible individuals, granting them the right to register on the platform. This method ensures that only authorized users can access the registration process. Tokens can be designed to expire and restrict access to certain features or content, increasing security and exclusivity.

Processed sensitive data (if applicable) and applicable restrictions or protective measures that fully take into account the nature of the data and the associated risks, such as strict purpose limitation, access restrictions (including access only for employees who have completed special training), records of access to the data, restrictions on disclosure, or additional security measures.

In order to use the XU platform, you must register by name on the platform in the registration area. Only persons who have been granted a license to use the XU platform may register. When registering, you must provide truthful information, and it is mandatory to use your real name.

Type of processing

XU: The data is processed automatically. We store the data securely and only transfer it via encrypted connections.

Purpose(s) for which the personal data is processed on behalf of the controller

Purposes of processing on behalf of the controller: Provision and operation of the learning platform, account management, course/webinar participation, timely reminders and follow-ups on behalf of the controller, reporting and administration functions as instructed. The DPA does not cover the processor's own purposes (e.g. marketing, product information, internal analysis).

Purposes of use of personal data on behalf of the controller may also include information about email addresses for comparison with the customer base. Provision and use of the XU platform for customers. Implementation of specific learning modules with the aim of further training in the area of responsibility.

Non-personal data includes the overall learning behavior of users on the XU platform, i.e. which content was learned and how often, registration rates for webinars, etc.

Duration of processing

The processing of personal data by the processor shall take place for the duration of the contractual relationship, including the contractually stipulated processing phase. Processing also includes the storage of personal data within the meaning of Art. 4 (2) GDPR. When processing by (sub)processors, the purpose, type and duration of the processing must also be specified. The following applies for the contract term plus the processing phase: After the end of the contract, the processor shall delete the personal data within 30 days at the latest or return it on instruction and confirm the deletion in writing. Backups shall be overwritten on a rolling basis and deleted after 90 days at the latest; system and security logs shall be deleted after 180 days at the latest (unless longer statutory retention obligations apply).

ANNEX II

List of subcontractors

EXPLANATION:

This appendix must be completed by sub-processors in the event of separate authorization (Clause 7.7(a), Option 1).

The controller has approved the use of the following subcontractors:

Status: 10/2025

Name	PostHog, Inc.
Street / No. / PO Box	2261 Market St PMB 4008
Postcode / Town	94114 San Francisco
Country	United States
Data location	EU (Frankfurt)
Brief description of the subcontractor's task	Product and usage analysis (events, funnels, experiments, optional session recording)
Type of personal data processed	• Data on user interactions (e.g. page views, clicks) • Browser and device information • IP addresses
Purpose of data processing	Analysis of user behavior within the LXP, optimization of the user experience, improvement of platform functionality

Name	Functional Software, Inc. dba Sentry
Street / No. / PF	45 Fremont Street, 8th Floor
Postcode / Town	94105 San Francisco
Country	United States
Data location	USA (EU option via relay if applicable)

Brief description of the subcontractor's task	Error and performance monitoring (error tracking, performance, session replay if applicable)
Type of personal data processed	• User IDs (for logged-in users during an error) • Technical data on errors (stack traces, browser information) • IP addresses
Purpose of data processing	Monitoring, identification and correction of errors within the LXP for stable operation

Name	Heroku, Inc.
Street / No. / Postcode	415 Mission Street, 3rd Floor (c/o Salesforce)
Postcode / City	94105 San Francisco
Country	United States
Data location	Europe
Brief description of the subcontractor's task	Platform-as-a-Service (app hosting, operation, databases)
Type of personal data processed	• All personal data of LXP • Logs with IP addresses and activity data
Purpose of data processing	Provision of a secure and scalable infrastructure for hosting and operating LXP

Name	Typeform S.L.
Street / No. / Postcode	Carrer Bac de Roda 163
Postcode / City	08018 Barcelona
Country	Spain
Data location	EU (Spain)

Brief description of the subcontractor's task	Online forms and surveys (data collection via web forms)
Type of personal data processed	• User IDs and contact information • Responses to surveys/forms (personal data possible)
Purpose of data processing	Creation and management of interactive surveys/forms for feedback and registration

Name	Microsoft Corporation (Azure)
Street / No. / Postcode	One Microsoft Way
Postcode / Town	98052-8300 Redmond, WA
Country	United States
Data location	EU (Germany West Central)
Brief description of the subcontractor's task	Cloud infrastructure and services (compute, storage, network)
Type of personal data processed	• All personal data of LXP • Logs and diagnostic data
Purpose of data processing	Provision of cloud services (hosting, databases, analytics) for LXP

Name	HubSpot, Inc.
Street / No. / Postcode	25 First Street, 2nd Floor
Postcode / City	02141 Cambridge, MA
Country	United States
Data location	EU Germany
Brief description of the subcontractor's task	CRM and marketing automation platform

Type of personal data processed	• User identifiers (email addresses) • Marketing engagement data (opens, clicks) • CRM data on interactions
Purpose of data processing	Management of marketing campaigns, communication and analysis of user interactions

Name	New Relic, Inc.
Street / No. / Postcode	188 Spear Street, Suite 1000
Postcode / City	94105 San Francisco
Country	United States
Data location	EU
Brief description of the subcontractor's task	Application performance monitoring (APM) and observability
Type of personal data processed	• Technical performance data • Anonymized session data • IP addresses in logs
Purpose of data processing	Monitoring LXP performance, identifying bottlenecks and optimizing the platform

Name	Infisical Inc.
Street / No. / Postcode	156 2nd St Unit 310
Postcode / City	94105 San Francisco
Country	United States
Data location	USA
Brief description of the subcontractor's task	Secrets management & secure administration of environment variables

Type of personal data processed	• User identifiers (e.g. email, API keys) • Authentication data (tokens) • IP addresses
Purpose of data processing	Secure management of secrets and configuration data for applications, CI/CD and infrastructure

Name	HashiCorp, Inc. (Terraform)
Street / No. / Postcode	101 Second Street, Suite 700
Postcode / City	94105 San Francisco
Country	United States
Data location	EU
Brief description of the subcontractor's task	Infrastructure-as-code platform (provisioning and management of cloud infrastructure)
Type of personal data processed	• User identifiers (e.g. email, API keys) • Infrastructure metadata (may indirectly contain personal data)
Purpose of data processing	Automated provisioning and management of infrastructure, compliance and monitoring

XU Group GmbH
Mehringdamm 33, 10961 Berlin,
registered in the commercial register of the Charlottenburg Local Court under HRB 172976 B, represented by the managing directors Dr Christopher Jahns and Nicole Gaiziunas-Jahns

www.xu.de
hallo@xu.de

APPENDIX IV

Technical and organizational measures (TOM)

in accordance with Article 32 EU GDPR, Section 64 BDSG

(Security of data processing)

Description of the technical and organizational security measures taken by the controller(s) (including any relevant certifications) to ensure an appropriate level of protection, considering the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons.

Pseudonymisation and encryption

(Art. 32(1)(a) GDPR, Art. 25(1) GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

We use Microsoft's cloud services in the area of infrastructure services. For this purpose, implementation procedures for pseudonymization and encryption are used directly on the platform. In addition, cryptographic procedures such as TLS and SSL are used for encryption. In databases, hard drives and data backups, additional encryption is implemented using RSA. A concept for general pseudonymization is currently being developed. This will allow personal data to be minimized in a meaningful way and its processing to be restricted in a data-efficient manner.

The ability to ensure the confidentiality, integrity, availability and resilience of systems and services related to processing on an ongoing basis

(Art. 32(1)(b) GDPR)

Confidentiality

Measures to ensure the confidentiality of systems and services designed to prevent unauthorized access to personal data.

Access control

Unauthorized persons must be denied access to rooms where personal data is processed. This is achieved through the following measures: security locks, a locking system with code lock, a manual locking system, alarm systems, and hazard reporting systems connected to a central control room. In addition, visits by external third parties are logged.

Key policy/key log

Key allocation is centrally managed and documented. The issuance of keys and who has access to which rooms is documented. In addition, employees and guests are required to carry their ID cards visibly. Access for external personnel is only permitted when accompanied by internal personnel. In addition, external personnel must sign a list. There is also a rule that the employee who is the last to leave the company premises on the current working day is obliged to lock the premises. If a key is lost, this is reported immediately and, thanks to the electronic system, the key can be blocked immediately. A key book is kept providing an overview of the history of access authorizations.

Access control

Unauthorized use of data processing systems must be prevented.

For this purpose, authentication is exclusively password-protected and uses two-factor authentication with a lockout routine in the event of too many incorrect entries. In addition, up-to-date antivirus protection programs and firewalls are used, with regular updates of both the programs and the signatures.

By appointing clearly responsible persons for updates and patch management, the respective installation version complies with the manufacturer's current recommendations.

Screensavers are password-protected for reactivation in order to ensure secure access even during business hours in the event of short or longer absences.

User profiles are created with different permissions and passwords. User accounts are monitored in accordance with the guidelines established for this purpose. The use of passwords is mandatory. Guidelines have been established for the creation of passwords. There is a limited number of failed login attempts.

Computer cases are locked. VPN technology is used for external access to internal systems. External interfaces such as USB sticks or CD-ROMs are blocked by default. Their contents cannot be transferred to the internal system. An intrusion detection system is used for this purpose. There are clear guidelines for the use of external data carriers. In addition, employees are instructed to maintain a clean desk policy.

Access control

Measures that ensure that those authorized to use a data processing system can only access the data for which they have access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

Many measures are used for this purpose, starting with a user authorization concept that promptly blocks/deletes the authorizations of employees who have left the company. User rights are managed by the system administrator and the respective project manager using the dual control principle. The number of administrators is reduced to the minimum necessary. In order to follow the principle of separation of functions, admin user rights are set up separately for the learning platform, CRM and other applications.

Of course, our password guidelines also apply here. Access to applications is logged and the data carriers are physically deleted before the data is reused.

If data carriers need to be destroyed, this process is carried out in accordance with regulations. Our company also uses document shredders. In addition, we also use service providers for document destruction. Data carriers and file folders are stored in lockable cabinets until they are destroyed.

Separation requirement

Measures that ensure that data collected for different purposes can be processed separately.

For this purpose, data is physically stored separately on separate systems or data carriers. Data records from different persons are logically separated and provided with purpose attributes/data fields. Assignment data is also separated from the actual data and pseudonymized.

The specifications in the authorization concept define the database rights. There is a separation between the production and test systems.

Integrity (Art. 32(1)(b) GDPR)

Measures to ensure the integrity of systems and services, which guarantee that personal data cannot be changed (unnoticed).

Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during transport or storage on data carriers.

In order to adequately ensure disclosure control, we use dedicated lines and VPN tunnels. Data is disclosed in anonymized or pseudonymized form. Passwords are also transmitted separately via alternative communication channels.

Email transmission (SSL/TLS) and email content (GPG/PGP or S/MIME) are encrypted. Data is transferred based on contractually agreed rights and obligations. Data carriers are clearly documented, and deletion periods are specified.

If necessary, data carriers are securely packaged for transport and transport personnel, or service providers are carefully selected. There are regulations for the secure transport of data carriers and for documenting data transport (recipients of data, time span of the planned transfer and deletion periods, etc.). If mobile data carriers are used, they include an encryption function.

Within the company, the WLAN is also encrypted (at least WPA 2). If sensitive data is to be passed on, this is also done in encrypted form using SFTP/PGP and the use of checksums/hash procedures when packing/unpacking files. A management system has been set up for the cryptographic keys.

To maintain an overview, a summary of regular retrieval and transmission processes has been created.

Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed in data processing systems.

To ensure this, we log the entry, modification and deletion of data in our system. Log control is carried out manually or automatically. Each user is assigned an individual username.

We also attach great importance to the secure storage of paper documents from which data has been transferred to the IT system.

In particular, we also rely on measures to gradually ensure traceability through an authorization concept.

Technical

Furthermore, various technical measures are used to ensure appropriate input control. Office 365 and Azure Logs (Admin Audit Log) are the leading systems when it comes to logging. SharePoint is used as the document management system. Log files are created to ensure the traceability of the deletion, modification and creation of personal data. These are versioned and old log files are stored in the recycle bin. The SSO learning platform is designed to prevent the (unintentional) overwriting of data.

Organizational

Organizational measures are also implemented to ensure appropriate input control. The only programs in which data can be entered, changed or deleted are the learning platform, in the browser, in Office 365 and in the apps. For the traceability of actions, each user receives their individual username.
the assignment of rights to enter, change or delete data is also done individually. The admin, XU, the learning management system and the customer decide on the assignment of rights. Access rights to the log files are assigned exclusively by the admin.

Availability and resilience (Art. 32(1)(b) GDPR)

It must be ensured that personal data is protected against (accidental) destruction or loss. On the other hand, the resilience of the systems and services involved in processing must be ensured in the long term.

Availability

Ensuring that personal data is permanently and unrestrictedly available and, in particular, available when needed. The ability to quickly restore the availability of personal data and access to it in the event of a physical or technical incident (Art. 32(1)(c) GDPR). Ensuring that the systems and services used can be quickly restored in the event of a malfunction.

Resilience

Ensuring that systems and services are designed in such a way that even occasional high loads or high continuous loads from processing remain manageable.

Technical

Surge protection is in place for the routers and firewall. The provider uses monitoring software to continuously monitor smooth data backup. This is contractually guaranteed. The installed virus protection and firewall are from Windows. Sufficient storage and performance capacities are available. These are regularly checked with a load and performance test. Backups and mirroring of hard drives are created in the cloud, where redundant data storage also takes place. Recovery tests are also carried out locally. An intrusion detection system (IDS) is used to detect attacks directed against a computer system or network.

Organizational

A data protection concept is implemented, which is, however, the responsibility of the provider. The same applies to the physically separate archiving of data backups in a secure location. The in-house data protection officer is responsible for training employees in the use of IT systems. Employees are regularly made aware of operational data protection issues. The administrators are responsible for monitoring the technical measures.

Order control

Order control is only applicable in the case of order data processing within the meaning of Section 62 of the new Federal Data Protection Act (BDSG) or Article 28 of the GDPR. It must be ensured that personal data processed on behalf of the customer is only processed in accordance with the instructions set out in the contract.

Technical

In the case of the role of the contractor in commissioned data processing, we fulfil the technical requirements.

Organizational

Contractors are carefully selected regarding data protection (this also applies to subcontractors). The contract is clearly drafted in accordance with Section 62 of the new BDSG and Article 28 of the GDPR. The contractor's data protection officer is specifically named, and their contact details are provided. The service provider's TOMs are checked for adequacy in accordance with Article 32(1) of the GDPR. Deletion periods are specified. A deletion concept is defined for the relevant areas. The standard AVV also ensures that the processing of contract data is carried out in accordance with instructions as a contractor. The client's rights to monitor the technical and organizational measures taken by the contractor (including subcontractors) are specified in writing. The client has the right to monitor the execution of the contract. An overview of the service providers and their services is available.

A procedure for regularly reviewing, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of processing. *(Art. 32(1)(d), Art. 25(1) GDPR)*

Technical and organizational measures have also been taken here to regularly review and assess the measures.

Technical

In addition to a technical review, the technical implementation is checked against certificate requirements. In addition, importance is attached to keeping the technology up to date.

Organizational

A data protection policy has been drawn up. Those responsible for the regular checks have been appointed. The measures are monitored and evaluated for effectiveness. If there is a need for action, this can thus be determined. Certifications are available.

XU Group GmbH
Mehringdamm 33, 10961 Berlin,
registered in the commercial register of the Charlottenburg Local Court under HRB 172976 B,
represented by the managing directors Dr Christopher Jahns and Nicole Gaiziunas-Jahns

www.xu.de hallo@xu.de