This English translation is for information purposes only. The original German text is the legally binding version in all respects. Original version: **https://xu.de/geschaeftsbedingungen/**

Order processing agreement

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" -

- Processor and Client hereinafter also referred to as "Parties" -

Standard Contractual Clauses

SECTION I

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 April 27, 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 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

a) The parties undertake not to amend the clauses except to supplement or update the information specified in the annexes.

b) This does not prevent the parties from incorporating the standard contractual clauses contained in these clauses into a more comprehensive contract and adding further clauses or additional guarantees, provided that these do not directly or indirectly contradict the clauses or restrict the fundamental rights or freedoms of the data subjects.

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

a) 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 – Optional

Catch-all clause

a) An entity 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) Upon completing and signing the appendices referred to in point (a), the acceding entity shall be treated as a party to these clauses and shall have the rights and obligations of a controller or processor as set out in Appendix I.

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

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of the processing

a) 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

7.1. 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 under the relevant law for reasons of public interest. The controller may give further instructions during the entire duration of the processing of personal data. These instructions shall always be documented.

b) 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 Union or Member State data protection law.

7.2 Purpose limitation

a) 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.

7.3 Duration of processing of personal data

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

7.4 Security of processing

a) The processor shall implement at least the technical and organizational measures listed in Annex III 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 "personal data breach").. When assessing the appropriate level of protection, the parties shall take into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of the processing, and the risks to the data subjects.

b) The processor shall grant its employees access to the personal data that is the subject of the processing 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.

7.5. Sensitive data

a) 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 offenses (hereinafter "sensitive data"), the processor shall apply special restrictions and/or additional safeguards.

7.6. 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 enable and assist in 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 take into account 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.

7.7. Use of Subprocessors

a) The processor is generally authorized by the controller to engage subprocessors 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) is/are engaged. The processor shall provide the controller with the necessary information to enable the controller 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 shall be by contract imposing substantially the same data protection obligations on the sub-processor as are imposed on the processor under these clauses. The processor shall ensure that the sub-processor complies with 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 Subcontracting 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 subprocessor with the obligations arising from the contract concluded with the processor. The processor shall notify the controller if the subprocessor fails to comply with its contractual obligations.

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

7.8. International data transfers

a) Any transfer of data by the processor to a third country or 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 subprocessor to carry out certain processing operations (on behalf of the controller) in accordance with Section 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

Support for 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 it has been authorized to do so by the controller.

b) Taking into account 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 point 8(b), the processor shall, taking into account the nature of the processing and the information available to it, assist the controller in fulfilling the following obligations:

    1. the obligation to carry out a data protection impact assessment on the planned processing operations (hereinafter referred to as "data protection impact assessment") where a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    2. the obligation to consult the competent supervisory authority or authorities prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    3. the obligation to ensure the accuracy of personal data by informing the controller without delay when it is found that the personal data processed by the controller is inaccurate or out of date;
    4. Obligations under Article 32 of Regulation (EU) 2016/679.

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

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 fulfill 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.

9.1. Breach of data protection in processing by the controller

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

a) immediately notify the competent supervisory authority or authorities of the personal data breach 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) 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:

   1) the nature of the personal data, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of records concerned;
   2) the likely consequences of the personal data breach;
   3) 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;

a) in accordance with the obligation laid down in Article 34 of Regulation (EU) 2016/679 to inform the data subject without undue 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.

9.2. 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 undue 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 where 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 Annex III any additional 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 it is unable to comply with these clauses for any reason.
b) The controller shall have the right to terminate the contract insofar as it concerns the processing of personal data under these clauses if
    1) the controller has suspended the processing of personal data by the processor pursuant to 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;

2) 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;

3) 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.

c) The Processor shall be entitled to terminate the Agreement insofar as it relates to the processing of personal data under these Clauses if the Controller insists on the fulfillment of its instructions after having been informed by the Processor that its instructions violate applicable legal provisions in accordance with Clause 7.1(b).

d) Upon termination of the contract, the Processor shall, at the choice of the Controller, 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 copies, unless there is a retention obligation 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 &amp; Co. KG*
Address:	*Ostengasse 14, 93047 Regensburg*
Name, position, and contact details:	*Christian Volkmer, Data Protection Officer*

APPENDIX 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.

Self-registration: With this method, individuals can register directly on the platform without a 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 safeguards that fully reflect the nature of the data and the risks involved, 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 and anonymously. 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

Customers and users agree that XU may contact them on behalf of the controller using the data provided during registration (e.g., name, email address). Reasons for contacting them may include: reminders about webinars booked on the platform, follow-up on webinars, evaluation of learning habits, reminders about uncompleted learning modules, monitoring of the learning process, news about the XU platform, and soliciting feedback.

The purposes of using 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., what content was learned and how often, registration rates for webinars, etc.

Duration of processing

2 months, duration of the pilot project. When processing by (sub)processors, the purpose, type, and duration of the processing must also be specified.

ANNEX III

Technical and organizational measures, including those to ensure data security

EXPLANATION:

The technical and organizational measures must be described in concrete terms; a general description is not sufficient.

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

See Annex "TOM"

ANNEX IV

List of subprocessors

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 subprocessors:

Subprocessors	**Service provided**	**Type of personal data processed**	**Purpose of data processing**
Administrative staff	Authentication services	- User identifiers (e.g., usernames, email addresses) - Authentication tokens - IP addresses	For authenticating users accessing the LXP and securely managing user sessions.
Posthog	Tracking and analysis	- User interaction data (e.g., page views, clicks); - Browser and device information - IP addresses	To analyze user behavior within the LXP, optimize the user experience, and improve platform functionality.
Sentry	Error monitoring and reporting	- User IDs (for logged-in users during an error) - Technical data on errors (e.g., stack traces, browser information) - IP addresses	To monitor, identify, and resolve errors within the LXP to ensure smooth and reliable operation of the platform.
Heroku	Cloud hosting services	- All personal data processed by the LXP, as Heroku hosts the entire platform - Logs that may contain IP addresses and user activity data	Providing a secure and scalable infrastructure for hosting your LXP to ensure availability and performance.
Typeform	Surveys and form creation	- User identifiers and contact information provided in forms - Responses to survey/form questions, which may contain personal data	To create and manage interactive surveys and forms for user feedback, registration, and other data collection activities within the LXP.
Azure	Cloud computing services	- Any personal data processed by the LXP when using Azure services for hosting, databases, or other cloud services - Logs and diagnostic data	Providing a range of cloud services, including hosting, databases, and analytics, to support the LXP's infrastructure and functionality.
HubSpot	Marketing and CRM services	- User identifiers such as email addresses - Marketing engagement data (e.g., email opens, clicks) - CRM data on user interactions and preferences	To manage marketing campaigns, email communications, and customer relationship activities, and to analyze user engagement and preferences.

New Relic	Performance monitoring	- Technical data on application performance - Anonymized user session data for performance analysis - IP addresses in logs	To monitor the performance of the LXP, identify bottlenecks or issues that affect the user experience, and improve the overall efficiency of the platform.

Appendix "TOM"

Technical and organizational measures (TOM)

pursuant to Article 32 EU GDPR, Section 64 BDSG-neu

(Security of data processing)

Pseudonymization 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 disks, 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, video surveillance, hazard warning systems connected to a central control room. In addition, visits by strangers are logged.

Video surveillance is a very sensitive issue, as it constitutes a significant intrusion into personal rights. Therefore, video surveillance always requires a legitimate legal basis. The exercise of domiciliary rights and the pursuit of legitimate interests (possible burglary) are reasons for using cameras. It is important to us that the purpose (for each video camera used) is documented so that the supervisory authority can understand the use of the cameras during an inspection.

The video surveillance system will be clearly indicated (e.g., with signs). Audio recordings are not permitted. For video surveillance, we document the following points: location of the cameras, location of the monitors, indication of video surveillance, type of recording, storage period, storage location.

Key policy/key log

Key allocation is managed and documented centrally. The issuance of keys, who has access to which rooms, and who has the master key is documented by name. In addition, employee and guest ID cards must be worn 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 requires the employee who is the last to leave the company premises on the current working day to lock up 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 to provide 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 anti-virus programs and firewalls are used, with regular updates of both the programs and 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 to which they have access rights, 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 duties, 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 data carriers are physically deleted before the data is reused.

If data carriers need to be destroyed, this process is also 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 that ensure that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which locations a transfer of personal data by data transmission facilities is intended.

In order to adequately ensure transfer control, we use dedicated lines and VPN tunnels. Data is transferred 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 on the basis of 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 documentation of 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 performed manually or automatically. Each user receives 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, the browser, Office 365, and the apps. To ensure the traceability of actions, each user is assigned an individual username. Rights to enter, change, or delete data are also assigned 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 hard disk mirroring are created in the cloud, where redundant data storage also takes place. Recovery tests are also performed locally. An intrusion detection system (IDS) is used to detect attacks directed against a computer system or network.

Organizational

A data protection concept is in place, which is, however, the responsibility of the provider. The same applies to the physically separate archiving of data backups in a secure location. The company's own data protection officer is responsible for training employees in the use of IT systems. Raising employee awareness of operational data protection is in the planning stage. 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 specified in the contract.

Technical

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

Organizational

Contractors are carefully selected with regard to data protection (this also applies to subcontractors). The contract is clearly drafted in accordance with §62 BDSG (German Federal Data Protection Act) and Art. 28 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 Art. 32 (1) GDPR. Deletion periods are specified. A deletion concept is currently being planned. Ensuring that order data processing is carried out in accordance with instructions as a contractor is also in the planning stage. 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 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. Furthermore, importance is attached to keeping the technology up to date.

Organizational

A data protection policy has been created. 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.