LXT General Contract Conditions for Transfer Toolbox

(Version: 11th May 2021)

§ 1 Subject of the contract and definitions

(1) The subject of the contract is the purchase of a licence for the platform Transfer Toolbox, developed by ourselves in cooperation with the Institute for Transfer Effectiveness (Institut für Transferwirksamkeit - ITW). This corporate e-learning software as ordered as part of a software as a service (SaaS) by you as a **commercial customer** (hereinafter "customer") in accordance with our quotation (hereinafter "**BI Quotation**")

(2) "Transfer Toolbox" is defined as the access to the e-learning platform provided by us and ordered by you to use. BI provides numerous other learning content, tools and systems for developing "Learning Professionals". BI therefore grants user-based licence rights for learners, whom the customer specifies and authorises to use.

(3) The terms listed below, which are used in these General Contract Conditions, have the following meaning:

- "**Customer**" is you as the contract partner of BI who is granted the use of Transfer Toolbox including the user licences according to the following conditions. "Customer" can be a natural person or a legal entity or other institution who allows the platform hereby provided by BI to be used by natural persons. Any companies associated with the customer in accordance with Article 15 German Companies Act (Aktiengesetz- AktG), do not participate as a "customer", that is as a contract partner. This is also the case if a users who are authorised by the customer belong to a company associated with the customer
- "**Users**" are all natural persons who are authorised to use Transfer Toolbox which has been provided by BI. Unless otherwise regulated, these are only Users who are either shareholders of the customer or others who are part of a service, working or training relationship or any other way subject to the customer's instructions when using Transfer Toolbox.
- "**Licence Agreement**" refers to the current **General Contract Conditions** for using Transfer Toolbox, **including annexes** in conjunction with the **BI Quotation**.
- "**Conditions of Use**" are the conditions for using Transfer Toolbox in your application in accordance with the annex, which should be read and observed by all users of Transfer Toolbox.

§ 2 Conclusion of Contract, Scope of the General LXT Contract Conditions for Transfer Toolbox

(1) When you order Transfer Toolbox in accordance with the BI quotation you conclude the licence agreement with:

Bildungsinnovator (eLearning Manufaktur GmbH) Erkrather Str. 401, 40231 Dusseldorf

e-mail: sales@bildungsinnovator.com
Phone: 0211 176074 80
Fax: 0211 545559 89
Commercial Register Dusseldorf District Court HRB 73424
Authorised Representative Managing Director: Adolf Rudolf Riegler

(2) Possible presentations of Transfer Toolbox by representatives of BI or on the BI websites or through other media are not a binding quotation from BI. On the contrary, after making contact with BI you will be given the opportunity to compile together a binding quotation for concluding the licence agreement with BI. **Only after you have received the agreed BI quotation with the General LXT Contract Conditions for Transfer Toolbox and you have accepted the BI quotation, does the licence agreement under the General LXT Contract Conditions for Transfer Toolbox come into force.**

(3) You will be provided with access to Transfer Toolbox by us in the learning platform LXT which is made available by us.

(4) Changes or amendments to the licence agreement through individual contractual agreements, as laid down in Article 305b German Civil Code (BGB) do not require any particular form. Otherwise changes and amendments require to be in **text form**. An oral revocation of this text form requirement is not permitted.

(5) If the BI quotation and these General Contract Conditions contain contradictory provisions for the same subject, the provision agreed in the BI quotation shall be considered as a special individual provision until the end of the contract.

(6) Possible **conditions of purchase/general terms and condition of the customer** are only valid when they have been expressly accepted by BI, whereby the conditions in this contract always have precedence in cases of conflicting performance conditions.

§ 3 Contract Duration and Termination

(1) The contractual relationship starts on the day that the operational Transfer Toolbox is made available.

(2) The licence agreement is valid indefinitely (lifetime licence).

(3) The right of the parties to this contract to **terminate for good cause** without observing any notice period remains unaffected. A good cause includes when the expressly regulated obligations from the licence agreement are grossly violated by a party to this contract, and particularly when insolvency proceedings are opened regarding the assets of the other party to this contract or the other contractual partner becomes insolvent or bankrupt. A further important cause exists when the customer gets into arrears with the payment of the fee or a substantial portion of the fee.

§ 4 Fee, fee when the number of users changes

(1) BI receives a one-off licence fee **in advance**, the amount being taken from the **BI Quotation** mentioned in Art. 1(1) and as agreed by the customer.

(2) An **individual adjustment or enhancement from LXT for the customer** does not form part of the current contract.

§ 5 Payment Terms

(1) The advance payment of the fee to be made to BI in accordance with Article 4 will be invoiced before Transfer Toolbox is made available. The payment is due 10 days at the latest after receipt of the invoice.

(2) **BI invoices** are **exclusively sent electronically**. The dispatch of the invoice by normal post is only undertaken upon special request in accordance with the statutory provisions.

§ 6 Provision of Transfer Toolbox, other services from BI and the customer's obligations to cooperate

(1) The XXX for using Transfer Toolbox will be provided by BI and protected against access by third parties. The internet access required for using Transfer Toolbox will be ensured by the customer.

(2) When registering as a Transfer Toolbox user, each user receives his personal access data either directly by e-mail or from the customer himself. The customer is obliged to share the e-mail address of the user which is required at registration and to give the user prior notice of this.

(3) The customer receives licence rights from BI. The customer therefore ensures that Transfer Toolbox is used according to its purpose (learning) and only in the user group specified by him. The customer will immediately inform of changes to the user group (e.g. changes in the e-mail addresses of Users). This obligation along with the personal duty of the user towards BI, which is attached as **Annex 1** as **LXT Conditions of Use,** must be adhered to. The LXT Conditions of Use are also accessible at any time on the LXT platform once it is accessible.

(4) BI attempts to have an availability rate for the platform of 99.5% as an annual average.

§ 7 Usage Rights

(1) BI grants the customer, subject to complete payment, the simple, non-transferable right to use Transfer Toolbox for an indefinite period. This also applies to future forms of usage of Transfer Toolbox.

(2) Should BI no longer make Transfer Toolbox available via the LXT platform, on request the customer can have a SCORM package provided to him. In this case you cannot pass the SCORM package provided to you to third parties not belonging to your user group.

(3) The user licence which you have acquired permits you and the persons who are specified by you as Users at the time of acquiring the user licence and named to us (e.g. members of your company or a certain organisational unit, who follow your instructions or are supervised by you) the personal and non-transferable use of Transfer Toolbox.

(4) Moreover, the **LXT Conditions of Use** for Transfer Toolbox attached to this contract as **Annex 1** and which were accessible on registration, apply to all Users.

(5) Usage rights, which may be taken up on the basis of lawful licences, in particular in accordance with Articles 60a ff German Copyright Act (UrhG), are not a part of this licence agreement and are not affected by the usage granted by LXT.

§ 8 Proprietary rights violations and indemnity obligations of the parties

(1) The Transfer Toolbox produced by BI in cooperation with the Institute for Transfer Effectiveness and the usage of the LXT platform granted, including relevant manuals and documentation, are subject to the protection of Art. 2 UrhG. The rights of third parties to the protected works remain unaffected. After prior notice and notwithstanding any possible claims for damages by the customer, BI is therefore permitted at any time to undertake changes to Transfer Toolbox, at its own expense, which guarantee that any infringements of proprietary rights of third parties through Transfer Toolbox or the use of the LXT platform are excluded.

(2) The customer is obliged to identify third-party rights which must be observed as a result of using Transfer Toolbox.

(3) The customer exempts BI, at the first request and at his own expense, from all third-party claims, insofar as the claim against BI by third parties is based on the alleged non-contractual or illegal use of Transfer Toolbox by the customer or the user. Conversely, BI exempts the customer from claims from third parties who claim an alleged proprietary rights violation by BI as provider of Transfer Toolbox. The parties are obliged to inform one another immediately about any asserted claims by third parties, which substantiate a reciprocal indemnity obligation.

§ 9 Guarantee, maintenance and services performance

(1) BI provides Transfer Toolbox in a suitable condition to fulfil the contractual usage and maintains this condition. The duty to upkeep does not include adapting Transfer Toolbox to changed usage conditions, technical and functional developments such as changes in the IT environment of the customer, in particular changes in hardware or the operating system, adaptation to the scope of functions of competing products or manufacturing compatibility with new data formats.

(2) Services from BI which are aimed at maintaining Transfer Toolbox technically up-to-date (maintenance services) or repairing faults, are rectified under the conditions mentioned in Art. 6(4).

§ 10 Liability

(1) BI is liable without restriction for **damages from injuries to life, body or health as well as for damages which are due to premeditation and gross negligence** on the part of BI or one of its vicarious agents. For damages which are due to a **minor negligent violation of essential contractual obligations**, BI is liable for the typically contractual foreseeable damage which can be typically expected. For **other instances of a minor negligent behaviour** Bi's liability is limited to EUR 25,000 per claim.

(2) In the **case of a loss of data**, BI is liable for the typical recovery expenses, which would have been incurred with the regular and risk-adequate production of backup files.

(3) Bi's liability without fault for defects in Transfer Toolbox, which already existed when the contract was concluded (Art. 536A (1)(1) BGB) is excluded.

(4) Liability as per the Product Liability Act remains unaffected.

§ 11 Data protection, data protection tasks for the customer.

(1) Personal data are processed when using Transfer Toolbox. Details can be found in **Information on Data Processing** (IDP) as per **Annex 3.** The IDP can also be viewed at any time in its current version on the LXT platform.

(2) The customer is the "Controller" and BI is the "Contract Processor"in accordance with Art. 28 GDPR, insofar as at least one of the following groups of people is affected by the data processing:

- Users of Transfer Toolbox as defined in Art 1(3);
- Users, who register personally via the registration data provided by BI as part of this contract.

The parties conclude the attached **"Contract on Order Processing"**, as **Annex 4** with its Appendices (TOM List, List of subcontractors, List of the technical and organisational measures taken with the DC operator IPB) to specify their data protection obligations, **in accordance with Art. 28(3) GDPR.**

(3) **Individual, chargeable data protection tasks** for the customer, which arise as part of processing the order, are governed by Art.4(3) of the Order Processing Contract (Annex 4) and must be ordered separately by the customer.

§ 12 Transferability of the rights from this contract, non-assignment clause, choice of law and agreement on jurisdiction of the court, severability clause

(1) Neither this contract nor any claims resulting from it can be transferred nor assigned to a third party without the prior written consent of the other party.

(2) German law applies.

(3) Place of jurisdiction for all disputes which result from this contract is Dusseldorf. BI retains the right to bring action against the customer at his registered office.

(4) Should individual provisions of this contract be or become partially or wholly ineffective or invalid, this does not affect the effectiveness of the contract as a whole. The parties undertake to substitute the ineffective or invalid provision with an effective provision which comes closest to the legal and commercial intent.

Annexes:

Annex 1: LXT Conditions of Use
Annex 3: Information on Data Processing (IDP)
Annex 4: Order Processing Contract (incl. Appendices: TOM list, Subcontractors)

LXT Conditions of Use

(Version: 05. January 2021)

The LXT platform is software that is run by us, **Bildungsinnovator, eLearning Manufaktur GmbH, Erkrather Strasse 401, 40231 Dusseldorf,** on a cloud server. LXT enables you as the user to produce learning content and to share it with others ("learners" and "authors"), who like you are authorised to use LXT by our customer (hereinafter "Your Company"). The setting-up of your user account on behalf of your company requires that you agree to the following conditions of use in accordance with the licence agreement for the LXT platform (hereinafter "Licence Agreement") which exists between us and your company.

Art. 1 Requirements for using the LXT platform

To use the LXT platform you receive your access data (registration data) from your company or directly from us , which authorise you for the personal and non-transferable use for the duration of our licence agreement with your company.

As the user you are obliged at the time of registration to provide true details about your person, especially regarding your membership of the group in your company who are authorised to use LXT.

It is forbidden for you to pass your access data to third parties and you must keep them safe. If you lose your access data you will only receive replacements via the e-mail address previously provided to us by your company.

Art. 2 Period of usage, termination of usage rights, blocking usage

The duration of your usage authorisation is dependent on the agreed duration of the licence agreement and requires that you are a member of your company's group of authorised users. Your usage authorisation therefore not only ceases at the latest with the termination of the LXT licence agreement, but also when you are no longer approved to use it by your company. That could, for example, be the case if you no longer work for the company.

In the case that we should ascertain that you are no longer authorised by your company to use LXT, we are entitled to block your user account immediately and without prior notice.

We are also entitled to block your user account when there is evidence that your account is being used by an unauthorised third party, or when the applicability or the security of the LXT platform we provide is compromised by your conduct or by the use of your user account.

Should there be a case of a blockage which you find to be unjustified, you should therefore get in touch with the contact person in your company who is responsible for us, who will then liaise with us.

Art. 3 Scope of usage rights, restricted usage of the LXT platform

When you register and agree to these conditions of use you receive a simple, non-transferable right to use the LXT platform, with the purpose of creating learning content within your company's group of authorised users or sharing it with other users.

We exclusively agree with your company the system requirements for using the LXT platform, any extension of the purpose of use or of the user group, on whose behalf we enable you to use this platform.

As the operator of the LXT platform, we reserve the right to temporarily suspend the operation of the platform if this is necessary for development, or to prevent a malfunction or security function. Any restriction in usage associated with that will be announced or indicated to your company, whose user group you are a member of.

Your company alone is authorised and obliged to explain to you the temporal, spatial or intended usage conditions of your personal usage rights.

Should there be a case of restricted usage, you should therefore initially get in touch with the contact person in your company who is responsible for us, who will then liaise with us.

Art. 4 Technical requirements, costs of using LXT

The technical requirements for using the LXT platform and any services and costs associated with its usage are solely agreed with your company, on whose behalf we enable you to personally use the LXT platform. There are no costs to you personally for using the LXT platform.

Art. 5 Guarantee, support services

We are constantly developing our LXT platform, which means that its functions – or respective parts of it – can change temporarily or permanently. If you should miss a previously-existing function, please have a contact person in your company who is responsible for us get in touch with us. It may be that the function is now located elsewhere as a result of developments.

Our contractual performance and guarantee obligations are part of the licence agreement with your company. In accordance with the current licence agreement between us your company is obliged to advise us immediately of any malfunctions or defects which arise from your usage of the LXT platform. So please get in touch immediately with the person in your company who is responsible for us.

Art. 6 Liability

Our liability to you as a direct user of the LXT platform is only so far as we are legally required. Insofar as we are legally liable to you, we bear unlimited liability for damages to life, body or health as well as damages which are due to our premeditated or gross negligent actions.

For minor negligence our liability is limited to typical and foreseeable damages. Our liability as per the Product Liability Act remains unaffected.

In the case of a loss of data, we are liable for the typical recovery expenses which would have been incurred with the regular and risk-adequate production of backup files.

Art. 7 Data protection, processing your personal data by a processor

We process personal data of the users in the course of your usage of LXT. All details of the data processing and your rights as the data subject can be found in **Information on Data Processing (IDP)** which can be downloaded from our LXT platform.

Art. 8 Changes to the conditions of use

We would like to point out that the present conditions can change afterwards, amongst other things in conjunction with modifications to the licence agreement concluded with your company (our customer). You will be advised should this case arise. You can find the currently valid conditions of use on our LXT platform, which are also available to download.

Annex:

Information on Data Processing (IDP)

LXT
Information on Data Processing

Version: 05.01.2021

Information on the collection of personal data

We are informing you here about the processing of personal data when using our “LXT” e-learning platform (“the platform”). In accordance with article 4(7) of the EU General Data Protection Regulation (GDPR) we, “Bildungsinnovator” (eLearning Manufaktur GmbH) are the controller, all contact details can be found in the Impressum of our Website).

Part 1: Data at every use of the platform

1. Browser data

(1) At every use of the platform, regardless of whether you use it as a learner, author, administrator or in another function, we collect personal data which your browser transfers to our server during the session. In these cases, we collect the following data which are technically required by us in order to make the platform usable and to ensure stability and security (legal basis is Article 6(1)(1) f GDPR):

- IP address;
- Date and time of the enquiry;
- Time difference to Greenwich Mean Time (GMT);
- Contents of the request (specific page);
- Access status/HTTP status code;
- Data volume transferred each time;
- Website from where the request came (referrer URL);
- Browser type and version;
- Language and version of browser software;
- The operating system used by your terminal device and its interface;
- Data volume transferred;
- Requesting telecommunications provider.
- Duration of request

(2) As a rule, we erase server logs after seven days, also later in individual cases, when concrete evidence provides us with justifiable suspicion that the platform was or will be used illegally, or an event has occurred which threatens the security or stability of the platform. In a case as per Art. 2 of this document the data are deleted after 90 days from the time that they are no longer required for clarifying the presumed event.

2. Cookies and Window.localStorage

(1) In addition to the above-mentioned data, during your use of the platform cookies and data are stored on your terminal device via the JavaScript function “Window.localStorage”. The platform uses both transient and persistent cookies, the scope and operating principles of which are explained below:

(2) The **transient cookies** used particularly include the session cookies, which store a session ID, with which different requests from your browser can be allocated to the joint session. That enables your computer to be identified again when you return to the platform. The session cookies are erased when you log out or close the browser.

The following transient cookies are used (please refer to the information in the relevant chapter for the details of each service):

JSESSIONID

Contents:	Session ID
Purpose(s)	Identification and allocation of the user during his current session in the platform
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	Session: This cookie is deleted when the browser is closed.

org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE

Contents:	Current language chosen by the user
Purpose(s)	Generating PDFs in the language chosen by the user
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	Session: This cookie is deleted when the browser is closed.

contentLanguage

Contents:	Preferred language as indicated by the user
Purpose(s)	Use of the platform in the language preferred by the user
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	Session: This cookie is deleted when the browser is closed.

contentLanguageSetByUserId

Contents:	Language set by the user
Purpose(s)	Use of the platform in the language chosen by the user
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	Session: This cookie is deleted when the browser is closed.

(3) The **persistent cookies** are automatically erased after a specified period, which can vary for each cookie. You can delete the cookies at any time in the security settings of your browser. The following persistent cookies are used:

_pk_id*

Contents:	Sets an ID for identifying the user
Purpose(s)	Helps to recognise a user for evaluations which are possible with Matomo (see Point 3)
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	13 months

_pk_ref*

Contents:	Attribute information
Purpose(s)	Internal evaluation as part of Matomo (see Point 3)
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	6 months

_pk_ses*

Contents:	Temporary data of a visit
Purpose(s)	For internal evaluations which are possible with Matomo (see Point 3)
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	30 minutes

SPRING_SECURITY_REMEMBER_ME_COOKIE

Contents:	Status of the setting of the “Remain logged in” function
Purpose(s)	Avoidance of unnecessary logins for the user
Collected by:	eLearning Manufaktur GmbH
Expiry/Erasure date	30 days

(4) Using the JavaScript technology “**Window.localStorage**” further categories of data are stored, in order to adapt the contents of the platform to the specific situation of the user and to make the use more comfortable and/or simpler. The functions contain, in particular, the following data categories:

- Activation/use of the function “Remain logged in”, with which a new login can be avoided at every browser restart;
- Storage of the login (more precisely: the authentication) of the user, in order not to have to repeat a login when using several tabs and windows.

- Storage of the part of the help tour already completed for training sessions, which makes it easier for beginners to use the platform, without repeatedly displaying online help;
- Activation/use of the editing mode in training sessions;
- Administration of the content held in the clipboard, in order to allow content to be exchanged and copied between different browser tabs and windows.

(5) You can configure your browser as you like and refuse to accept third-party cookies. The platform cannot be used without using any cookies and without using Window.localStorage.

3. Tracking the browser used via Matomo

(1) In order to trace with which browser the platform is used, we track the hits on the homepage of the platform by all users with the open source system "Matomo" (https://matomo.org/, formerly "Piwik"), which is also hosted on our own servers. In so doing we collect IP addresses, which have the last three digits removed. Matomo uses both transient and persistent cookies for the tracking stated and for the purposes cited. The legal basis for this usage is our interest in having a usable platform which is as fault-free as possible (Art. 6 (1)(1) f GDPR).

(2) You can veto the collection of the specified data by opening the link below. In this case a so-called opt-out cookie will be stored in your browser, as a result of which Matomo will not collect any session data. Note: If you delete the mentioned cookie or all of your cookies, you have to set the mentioned cookie again.

https://piwik.elearning-manufaktur.com/index.php?module=CoreAdminHome&action=optOut&language=de

The data collected via Matomo are not routinely deleted.

4. Contacting us

If you contact us directly (e.g. via the e-mail address support@bildungsinnovator.com), the data provided by you (e.g. your name, your e-mail address and other data such as your telephone number) will be processed by us, in order to deal with your concerns. The legal basis for this processing is the requirement to fulfil your request in accordance with Art. 6(1)(1) b GDPR. Depending on the request, we have to store your data for a certain period, in order to comply with our accountability; legal basis for this storage is Art. 6(1)(1) c GDPR.

5. Categories of personal data collected regardless of user rights

The following data categories of all users, regardless of the user role or permitted user rights (so especially of learner users), are processed when using the platform:

- Time of every individual **login and login attempt**;
- **Authorisations** of your user account and their changes incl. time stamp;
- **Learning progress data**

i. **Call-ups of content** (“Cards”): Name of the card, time stamp of the call-up and your user ID;

ii. **all of your answers to quiz questions**: when you answered which question(s) and whether the relevant answer was right or wrong;

iii. **Answers** as **part** of **quiz collections**: the answers given by you, the points achieved as part of the quiz collection as well as the time required to complete the whole quiz collection.

iv. **Certificates** you have **achieved**.

- The **bookmarks** you have saved;
- **Your assessments** of cards, including assessment text, where applicable;
- Cards shared by you with others and by others with you, including the time stamp of sharing;
- **Tasks delegated to you and by you** including the date and time of delegating and comments on every task;
- **Questions asked by you to experts.**

6. Categories of collected personal data depending on the user role or user rights

The following additional categories of personal data are processed in the platform depending on the respective user role or the rights granted to a user:

Granted permission	Processed data categories	Authorised user
“Use task management”	Which tasks were delegated when by which user to which user	User with the permission “Use task management”
“Set up content permissions”	Which user set up or erased rights for what content	Bildungsinnovator administrators
“View reporting”	Which user has created/downloaded which reports with which parameters and when	Bildungsinnovator administrators
“Use recycle bin”	Which content was erased by which user and when	All users of an installation
“Create, update, erase User / User Groups / Roles”	Every change to a user permission	Bildungsinnovator administrators
“Use templates”	Which user saved which template and when	Every user with “Use templates”
“Set up content permissions”	Every change to content permissions is logged.	Bildungsinnovator administrators
“Use skill sets”	Authorisation-relevant changes (adding collections or user groups to a skill set)	Bildungsinnovator administrators

Part 2: Which user can view which data

In this section we explain to you which other users in the platform can access your data. As the technical administrators of the installation can access all personal data (and also have to be able to do that to ensure the faultless functioning of the platform), this is not discussed any further.

1. Your answers to quiz questions

Users with access to user administration can see if you have answered a particular question right or wrong, as well as the time stamp of your first and your last answer to this question.

2. Certificates you have achieved

Users with the authorisation “View reporting” can view which certificates you have achieved and when.

3. Whom you can find within the platform and when

- Any other learners can find your name and e-mail address, when you want to share a learning card with anyone else, when they type in the first three letters of your first name and surname.
- Users with the authorisation “Use task management” can also use the mentioned search function in ‘a’ to assign (or: delegate) tasks to others.

4. You as an Expert

If you are asked a question as an expert, your name is visible to all users in connection with the question(s) put to you, so long as you answer the question. In contrast to learners, who can ask you questions anonymously, you cannot answer anonymously.

Part 3: Storage periods and your rights

1. If and as far as not otherwise described, the data categories mentioned in this document will basically be stored until the platform is erased. You do of course have the right of erasure according to the following guidelines.

2. Irrespective of how you use the platform, as the data subject you have the following rights against us with regard to the personal data concerning you:

- Right to information;
- Right to rectification or erasure;
- Right to restriction of processing;
- Right to objection to the processing;
- Right to data portability;

3. You also have the right to lodge a complaint with a data protection supervisory authority about the processing of your personal data by us. Before you do that, we recommend, however, that you get in touch with us.

4. You can reach our data protection officer with the following contact details:

Innara UG (haftungsbeschränkt) & Co. KG
Frank Stiegler
Martin May Strasse 10
60594 Frankfurt

Phone: +49 69 6642699-00
Fax: +49 69 6642699-09
e-mail: datenschutz@bildungsinnovator.de (Public PGP Key, S/MIME-Zertifikat)

Appendix 4: Agreement on contract processing as defined in art. 28 para. 3 GDPR

(Version: 23.04.2021)

Introduction

This Appendix, including its Annexes, makes specific the data protection obligations of the parties to the agreement arising from the contractual services provided by the contractor (BI – eLearning Manufaktur GmbH) for the purchaser (customer) within the context of making the platform "LXT" (formerly "Learning cards") available. It applies to all activities associated with this purpose, during the implementation of which employees of the contractor or a person acting on behalf of the contractor process the customer's personal data ("data"). This agreement replaces any prior agreements on data protection between the parties to the contract.

If or to the extent that an agreement on contract data processing under the terms of § 11 GDPR in the version applicable up to 24.05.2018 had previously been concluded, the said agreement is replaced by this one.

Headings in this document are for reference purposes only.

§ 1 Object and duration of contract processing

(1) The object and duration of the contract and the type and purpose of processing are set out in the main contract. The following data in particular are an integral part of the data processing:

Type and purpose of data processing	Data categories included	Categories of data subjects
Operation of the "LXT" platform as a Cloud platform	• Users' master data: Name, Email address • Users' account data: roles, authorisations, user names, hierarchies, logins (time and duration of login) • Learning status data: content completed, test results/final grades • Communication data: E-mails, chats (metadata such as content)	• Customer's employees • Platform users • Contractor's administrators

Contractor's support services provided on the customer's instructions	As specified by the customer, probably any regular contact and learning progress data	As specified by the customer, probably any regular employees of the customer and LXT users

The term of this Appendix is aligned with the term of the main contract, unless more far-reaching obligations arise from the provisions of this Appendix.

(2) The contractually agreed data processing tasks shall take place exclusively in a member state of the European Union or in another signatory state to the European Economic Area Treaty. If or to the extent that there is to be any derogation from this procedure, the special conditions of art. 44 et seq. GDPR must be met, and the customer must be notified of the respective change at least 30 (thirty) days in advance.

§ 2 Customer's responsibility

(1) The contractor shall process personal data on behalf of the customer in accordance with art. 28 GDPR. The customer is the sole data controller within the meaning of art. 4 no. 7 GDPR.

(2) The instructions necessary for the contractor's activity within the context of contract processing shall be determined by the customer initially through the contract, and may be amended, added to or replaced thereafter by individual instructions sent in writing to the department designated by the contractor ("individual instruction"). Verbal instructions must be confirmed immediately in writing or in electronic text form.

§ 3 Contractor's duties

(1) **Processing according to instructions**

The contractor may process the data of data subjects only within the framework of the contract and the customer's instructions unless an exemption exists within the meaning of art. 28 para. 3 letter a) GDPR. The contractor shall inform the customer immediately if he believes that an instruction contravenes applicable laws. The contractor may postpone implementation of the instruction until it is either confirmed or amended by the customer.

(2) **Taking technical and organisational measures ("TOM")**

The contractor shall arrange the internal company organisation within his sphere of responsibility in such a way that it complies with the special requirements of data protection. For the reasonable protection of the customer's data, he shall take TOM that satisfy the requirements of arts. 24, 32, 5 GDPR. The contractor may further develop TOM on an ongoing basis in order to take technical progress into account. He may thus take adequate alternative measures so long as these do not fall below the level of protection offered by the measures specified in Annex 1 to this Appendix. Major changes must be documented.

(3) **Support for the customer in implementing the rights of data subjects**

The contractor shall support the customer to a reasonable extent in satisfying the enquiries and claims of data subjects in accordance with chapter III of the GDPR and in fulfilling the duties set out in arts. 33 to 36 GDPR. If any claim is pursued against the customer by a data subject under the terms of art. 82 GDPR, the contractor undertakes to support the customer to a reasonable extent in defending the claim.

(4) **Undertaking given by all persons processing data**

Within the framework of fulfilling his contract, in accordance with art. 28 paras. 3 sentence 2 letter b, 29, 32 para. 4 GDPR, the contractor shall engage exclusively persons who have given a confidentiality undertaking and have been familiarised in advance with the data protection provisions relevant to them. The contractor and any person reporting to him with access to personal data may process these data exclusively in accordance with the customer's instructions, including the authorisations granted in this contract unless they have a legal duty to process them.

(5) **Notification in the event of breaches of data protection**

The contractor shall notify the customer immediately if he becomes aware of breaches of the customer's personal data protection. He shall take the necessary steps to secure the data and reduce any possible adverse consequences for the data subjects, and will consult the customer on this matter without delay.

(6) **Drawing attention to measures taken by the supervisory authority**

The contractor shall inform the customer about checks made and actions taken by the supervisory authority if these relate to the services which are the object of the contract, and shall agree the procedure with him. This also applies if a competent authority is investigating in the course of regulatory or criminal proceedings with regard to the contract processing of personal data by the contractor.

(7) **Compliance-inspection procedure**

The contractor shall regularly inspect the internal processes and their TOM to guarantee that they are in accordance with the requirements of applicable data protection law.

(8) **Surrender/erasure of data after the end of the contract**

Data, data supports and all other materials must be either surrendered or erased after the end of the contract at the request of the customer.

(9) **Exclusion of the right to retain data defence**

The defence of the right to retain data within the meaning of § 273 BGB (German Civil Code) is excluded in respect of the personal data processed by the contractor within the framework of this agreement.

(10) **Data protection officer**

The contract processer has appointed Innara UG & Co. KG, Martin-May-Straße 10, 60594 Frankfurt, Mr Frank Stiegler (tel.: +49 69 664269911, Email: datenschutz@bildungsinnovator.com) as external data protection officer.

§ 4 Customer's duties

(1) **Notification of errors**

The customer must inform the contractor immediately and in full if he notices errors or irregularities related to the provisions of data protection in the contractual results.

(2) **Support for the customer in implementing the rights of data subjects**

Should any claims under art. 82 GDPR be pursued against the customer by a data subject, § 3 para. 3 sentence 2 of this contract applies accordingly.

(3) **Payment for the contractor's data protection services**

The customer must pay the contractor for the activities arising within the framework of this agreement on contract processing in accordance with the agreed rates, or otherwise in accordance with standard rates, to the extent that these are provided individually for the customer and have not become necessary due to a culpable infringement by the contractor of his duties under the terms of this agreement. "Activities" as stated in this sentence 1 include in particular carrying out or assisting with the following activities:

a) Audits by the customer on the contractor's premises if, or to the extent that, no substantial breaches of data protection are established during these;

b) Enquiries by data subjects directed at either the contractor directly or at the customer if and to the extent that the contractor assists with these;

c) Any restriction, erasure etc. of data requested by the customer, provided it is technically impossible for him to undertake the desired data processing himself with the solution made available by the contractor;

d) Any assistance with data protection impact assessments requested by the customer;

e) Notifications to the customer triggered by unlawful data protection instructions issued by the customer;

f) Assistance by the contractor (including any disruption of operating processes on his premises) which becomes necessary due to searches carried out by public bodies on his premises relative to the customer's data;

g) Assistance in the customer's notifications under art. 33 GDPR and, in the case of notifications by data subjects, under art. 34 GDPR if or to the extent that the contractor did not culpably cause the reason for the obligation to report or notify.

§ 5 Quality assurance

(1) The contractor shall prove to the customer that the duties laid down in this contract have been fulfilled by providing the following documents:

a) written appointment of the data protection officer who will provide evidence of their activities in accordance with art. 38, 39 GDPR;

b) presentation of the confidentiality agreement in accordance with art. 28 para. 3 sentence 2 letter b, 29. 32 para. 4 GDPR;

c) current certificates, reports or extracts from reports by independent authorities (eg. financial auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors);

d) suitable certification by IT security or data protection audit (eg. in accordance with TISAX).

(2) **Data protection audits**

If and to the extent that the contractor cannot prove compliance with the measures to be taken under the terms of this agreement in accordance with this para. 1, the customer has the right to make sure that the TOMs to be taken by the contractor in his business operation in accordance with this agreement have been implemented by carrying out checks in consultation with the contractor. The contractor may make the tests generally necessary for this purpose dependent on prior warning with reasonable advance notice and on the signature of a confidentiality declaration in respect of the data belonging to other clients. If and to the extent that these checks cannot enable the customer to gain access to any personal data or data belonging to the contractor's other business partners which have to be treated as confidential for a different reason, the customer may carry out the respective checking actions himself. If these checks process data that do not belong to the customer's area of contract data, the customer must arrange for such checks to be carried out by a third party who has an obligation to preserve confidentiality under the terms of a code of professional conduct, eg. a lawyer or auditor. If the organisation appointed by the customer to carry out the checks is a competitor of the contractor or of one or more of his clients, or cannot demonstrate a level of data protection and IT security that corresponds to this contract, the contractor may decline to accept this inspector, and the customer must then select a different inspector who does not have these characteristics.

§ 6 Sub-contracting conditions

(1) The contractor also uses other enterprises for the provision of (part of-) the services ("sub-contractors"). Sub-contractors are deemed to be "processing sub-contractors" if/to the extent that they process personal data on behalf of the contractor, however not if they process personal data at the time of providing services to the contractor merely

a) as an additional service whilst ensuring the confidentiality, availability, integrity and resilience of the hardware and software of **data processing systems** (eg. by providing telecommunication services, postal/transport services, maintenance or user support services) or

b) simply have the possibility of access to the customer's personal data but have given a **contractual undertaking not to make use of such access** (eg. as providers of computer centre premises and support services, such as protection from natural hazards and an uninterruptable power supply).

Sub-contractors who are not processing sub-contractors under this ruling are described in this document as "suppliers".

(2) The contractor may at his own discretion engage and replace suppliers and terminate contracts with them provided that the duties of the contractor under the terms of this contract are fulfilled. He must present the customer with a list of suppliers engaged if the customer so wishes.

(3) **The contractor may engage processing sub-contractors only with the express prior, documented permission of the customer.** The customer grants permission to engage the processing sub-contractors listed in Annex 2 to this Appendix within the framework of conclusion of this contract. Any change of processing sub-contractor is subject to the prior, documented permission of the customer which he may not, however, refuse without a substantial reason under data protection law.

(4) Regardless of whether a sub-contractor is a processing sub-contractor or not, the contractor must ensure that reasonable protection and reasonable security is provided for the customer's processed data through contractual agreements and effective control measures.

§ 7 Duties to provide information, clause requiring the written form, choice of law

(1) If the customer's data should be put at risk by the contractor due to attachment or seizure, insolvency or settlement procedures or due to other events or actions taken by third parties, the contractor must inform the customer accordingly without delay. The contractor will inform all persons with responsibility in this connection that data sovereignty rests exclusively with the customer as the data controller within the meaning of the GDPR.

(2) Any amendments or additions to this Appendix and all components of it, including any assurances given by the contractor, must be in writing and must make express reference to the fact that they constitute an amendment and/or addition to these conditions. This also applies to any waiver of the requirement for the written form.

(3) In the event of any contradictions, the data protection provisions in this Appendix take precedence over the provisions of the main contract. Should any individual parts of this Appendix be invalid, this shall not affect the validity of the rest of the Appendix.

Annexes to this document:

Annex 1: List of technical and organisational measures taken
Annex 2: List of processing sub-contractors used

Annex 3: List of technical and organisational measures taken by Computer Centre operator IPB Internet Provider in Berlin GmbH

Annex 1

Technical and organisational measures

in accordance with arts. 24, 32 GDPR (Version: 23.04.2021)

The measures set out in this document shall be taken by the contractor when providing his contractual activities for the customer for the purpose of data protection ("Data" in this Annex also means personal data as defined in art. 4 no. 1 GDPR).

Independently of the measures described here, the contractor is certified to the TISAX standard (a standard to prove IT security measures), therefore also takes further data security measures which will be made available to the customer on request.

1. Confidentiality

(art. 32 para. 1 letter b GDPR)

Summary of measures to monitor entry and access measures

There are three different types of data processing systems:

- (one or more) servers in one or more computer centres ("CC") ("the server");
- the contractor's "mobile terminals", i.e. terminals with a mobile operating system (eg. iOS and Android);
- the contractor's "stationary terminals", i.e. all terminals which are not mobile terminals.

Server location Heinlein Support GmbH ("Heinlein")

One or more servers on which LXT installations are operated will be made available by the sub-contractor Heinlein Support GmbH ("Heinlein"), who for their part will use the sub-contractors IPB Internet Provider Berlin GmbH ("IPB"). Both the CC operators named above are certified to ISO 27001.

Heinlein does not primarily process data under contract, but makes available first and foremost hardware and CC capacity (site protected against natural hazards with uninterruptable power supply and robust internet connection) as well as support services, for instance exchanging defective hard discs, providing necessary server new starts and similar.

The CCs used by Heinlein for this purpose are located in Berlin.

Location of Amazon Web Services, Inc. (“AWS”) server

In principle similarly to Heinlein/IPB, AWS makes server capacity available on which LXT installations can be operated, also certified to ISO 27001.

Location of Dusseldorf branch

The offices in Dusseldorf are located on the 2nd floor of the “Factory Campus” at Erkrather Straße 401 in Dusseldorf, a fenced building complex equipped with lighting controlled by movement sensors, containing the offices of several companies including the contractor. Most of the ground floor side doors and windows are equipped with roller shutters which can be pulled down manually outside of office hours. The building is locked outside normal office hours, and can be accessed during normal office hours by means of a building entry key which is handed to staff of all the companies in the Factory Campus and does not open any doors apart from the building entrances. The building has CCTV in various places (corridors, entrance hall, shared spaces). The contractor’s offices can be accessed only via transponder devices which are handed out exclusively to the contractor’s staff. Unaccompanied visitors must register at the central Reception desk for the Factory Campus, to which they can gain access by ringing the doorbell at the entrance, and Reception staff then grant them access. To gain access to the contractor’s offices, visitors have to be collected from Reception by the contractor’s staff.

Location of Kleve branch

The offices of the Kleve branch are located in a building at Schloßtorstraße 39 in Kleve, which only houses the contractor’s offices. The land is fenced, and the building is locked outside normal office hours and secured by an alarm system connected to various movement sensors in the building which triggers an alarm at an external security firm. Movement sensors on the outside of the building control lights on the building outside normal working hours. Most of the ground floor side doors and windows are equipped with roller shutters which can be pulled down manually outside office hours. During normal office hours, the building can be accessed with an electric door-opening device which is only handed to the contractors’ staff who work at the Kleve site plus legal representatives of the company, if applicable.

1.1. Access control

Aim: Processing systems used to process personal data must be secured against unauthorised access.

Measures taken in the CC:

Situation at IPB
This CC operator is certified to ISO 27001; the certificate can be downloaded at https://www.ipb.de/company/certifications.html. The CC operator takes TOM in accordance with the document appended as Annex 3.
Situation at AWS
Measures are taken in accordance with ISO 27001 certification (can be downloaded at https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf)

Measures taken at the Dusseldorf branch:

Area	Situation
Land	• Fenced building • Movement sensor-controlled lighting on the site
Building	• The building's windows and side doors are secured by roller shutters outside office hours. • Doors to the building are locked outside office hours. The corresponding keys which do not open any doors apart from the entrances to the building, are handed to staff belonging to all the companies on the Factory Campus.
Areas in the building accessible to all companies	• The building has CCTV in various places (corridors, entrance hall, shared spaces). • A central Reception area is set up as the first point of contact for all visitors.
Contractor's offices	• The offices can only be accessed via transponder devices which are handed out exclusively to the contractor's staff. • To gain access to the contractor's offices, visitors have to be collected from Reception by the contractor's staff.

1.2. Access control

Aim: the processing systems described above must be secured against unauthorised use.

Measures taken in the CC:

situation at IPB (sub-contractor of Heinlein)
All Admin accesses are secured by personal SSH keys and access is possible only from specified IP addresses.

Situation at AWS
All Admin accesses are secured by personal SSH keys and access is possible only from specified IP addresses.

Measures taken in the branches:

Area	Situation
Stationary terminals	• Hard disc encryption • All employees and vicarious agents of the contractor must log in to each server via a personal authentication code (SSH with asymmetric encryption) before they can access any data. • Authentication data must have the level of complexity corresponding to the state of the art. • The operating systems of the terminals used will be kept at the most recent security update status. • Use of firewall • The respective users of virtual workstations will be locked out after an absence of at least 5 minutes.
Mobile terminals	• With the exception of any data which may be sent from the customer by email, no data will be stored on mobile terminals. • Mobile terminals will not be used for logins to servers. • The operating systems of the terminals used will be kept at the most recent security update status.
External data supports	• External data supports may not be used to store data.
Paper documents	• Paper documents containing data will be stored in locked metal boxes and either erased and/or destroyed before or at the time of their disposal in compliance with DIN 66399 Category 3.
Data supports	• Data supports will be either erased and/or destroyed before or at the time of their disposal in compliance with DIN 66399 Category 3. • Before a data support is re-used for a different purpose, the data on it will be erased and overwritten via Secure Erase.
Networks (LAN, WLAN)	• At the Dusseldorf branch, a self-managed LAN and a self-managed password-protected WLAN are used. • At the Kleve branch, a LAN network and two separate, password-protected, encrypted WLANS are used, one for company purposes, and one for visitors and guests. All the networks described here are accessible only to the contractor.

Miscellaneous	• Data on the platform are basically and primarily processed on the server. On stationary or mobile terminals, they are basically only processed temporarily for as long as necessary for specific contract activities. • Two cases form exceptions to the principle set out above: 1. The customer sends data to the contractor by email. 2. For the purposes of error correction or support, changes are required to the client database in which all the customer's user data are stored. The contractor's relevant employee then copies the aforementioned database onto the computer he is using and leaves it stored there until a further instruction is received from the customer, so that he can answer connection questions. The customer may request erasure of the data at any time. • A Clean Desk Policy exists throughout the company, under which the data support and all documents containing data are protected against unauthorised access, both in analogue form (eg. via lockable cabinets) and digital form (eg. via desktop lockout instruction and lockout function when not in use).

1.3. Access control

Aim: The guarantee must be given that the person authorised to use a data processing system can access only the data for which they have access authorisation, and that personal data cannot be read, copied, altered or removed during processing, use and after storage without authorisation.

Situation:

As necessary for the respective activity, the contractor's employees (eg. administrators, authors and trainers) have access to data. The measures described below will be taken by the contractor. The measures taken or to be taken by the customer lie within the scope of his responsibility.

Measures taken:

Area	Situation
Allocation of access rights (rights/role concept)	• Users can and may access data only via specific personal accounts.

	• Authorisations are given as a function of the necessity of the respective access. Access authorisations for all the contractor's staff working on fulfilment of the contract are based on the *principle of least privilege*, are regularly monitored and are adjusted immediately to changing situations (assignment of rights to new employees, deletion/blocking of rights of departing employees and the adjustment of rights for employees with changing work profiles).
Access log	• All read and write accesses to data are logged to the specific user.

1.4. Segregation control

Aim: There must be a guarantee that data collected for different purposes (digital or physical) can be processed separately.

Measures taken:

Area	Situation
Segregation of data belonging to other customers	The database and files are stored in accordance with the customer's instructions in segregated directories or on separate servers with separate authorisations.
Segregation of live and test data	Physical separation of data in the live application and in test applications (if so requested by the customer).

1.5. Pseudonymisation

Aim: The measures listed here provide the guarantee that personal data can no longer be attributed to a data subject without entering additional information.

Situation:

No pseudonymisation or anonymisation measures are used. Use of the platform is voluntary, and the contractor has no authority to decide which users contribute what data. Users may delete their accounts in full at any time.

Measures taken:

Area	Situation
Data for development/support purposes	Anonymised or pseudonymised data are used by developers where possible for the support and development of new features.

2. Integrity

(Art. 32 para. 1 letter b GDPR)

2.1. Data transmission control

Aim: To guarantee that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data supports, and that it is possible to establish where personal data are to be transmitted by data transmission equipment.

Situation:

Data on the platform are exported or transmitted by the contractor only after being instructed to do so by the customer, unless the export or transmission is necessary to fulfil the contractor's duties to the customer. The export and transmission of data by the customer lie within his scope of responsibility. Measures are described below which safeguard and log access by certain clients to the server.

Measures taken:

Area	Situation
Data transfer from/to the server	Any data exchange is protected by the use of encryption and VPN or SSH technologies in accordance with the latest state of the art. The contractor will not send either personal data or access data such as passwords via unencrypted connections.
Safeguarding electronic transmission	If files are transmitted electronically in accordance with the customer's instructions, the following measures are taken, depending on content: • Password protected Zip-Archive • One-timedownload links with non-guessable URL • Time-limited download option

2.2. Input control

Aim: To guarantee that it is possible to check and establish retrospectively whether and by whom personal data were entered in data processing systems, or altered or removed.

Measures taken:

Area	Situation
Alterations with security relevance	Data alterations categorised as relevant to security (eg. alterations in access authorisations, changes of user master data such as name or email address and the password used) are logged centrally (not tamper-proof). Only the contractor's administrators routinely have access to these log data.
Other alterations	The platform logs any and all alterations to data for the purpose of providing the contractual services, and in particular to make analysis possible in cases of error. The customer has the right to choose whether this should happen.
All read/write accesses to data	Subject to an instruction to the contrary by the customer, all read and write data accesses are logged specifically to the user.

3. Availability and resilience

(art. 32 para. 1 letter b GDPR)

3.1. Availability monitoring

Aim: To guarantee that personal data are protected against accidental destruction or loss.

Measures taken:

Area	Situation
Data backups	All the customer's personal data are backed up in accordance with a system with a mix of full and incremental back-ups and a rotation of maximum one year; this mix reflects the current status of the data at the respective time of creation of the backup. Only the contractor's system administrators have access to the aforesaid backups.

3.2. Reliability

Aim: To guarantee that all functions of the system are available and any malfunctions occurring are reported

Measures taken:

Area	Situation
Server monitoring	• Automatic monitoring systems for critical systems (errors in data storage, file system, availability of systems) • Errors and warnings occurring are logged.
Server reliability measures	• Uninterruptable power supply (UPS) • Emergency power diesel generator • Fire and smoke alarm system • Air-conditioning in server rooms

3.3. Data integrity

Aim: To guarantee that stored personal data cannot be corrupted by malfunctioning of the system

Measures taken:

Area	Situation
Server: RAID 1	RAID-1 technology is implemented on the server to compensate for hard disc malfunctioning.

3.4. Restorability (systems)

Aim: To guarantee that the systems implemented can be restored in the event of a failure

Situation:

The robust operation of the platform is safeguarded through monitoring. Incidents will be notified first to the contractor and immediately afterwards to the customer. The contractor's support team regards incidents compromising operation of the platform as high priority, and the processes used in this respect are part of the aforementioned TISAX certification.

Measures taken:

Area	Situation
Backup und Recovery	The database and application files are backed up daily on a dedicated server with full and incremental backups which overwrite one another using complex logic in order to retain the greatest possible availability, including of older data, without taking up unnecessary storage space for backups. Data are stored for a minimum of 7 days. A monthly check is carried out to ensure that the backups have been correctly created.
Incident Management	Contact is made with the hosting provider for the purpose of exchanging defective hardware and uploading the latest backups.

4. Procedure for regular checking, assessment and evaluation

(art. 32 para. 1 letter d GDPR; art. 25 para. 1 GDPR)

4.1. Data protection management (DPM)

Aim: To guarantee that personal data processed under contract can only be processed in accordance with the customer's instructions

Measures taken:

Area	Situation
TISAX certification	The contractor is TISAX certified (Trusted Information Security Assessment Exchange, an IT security standard established by the automotive industry, derived from ISO 27001) and regularly checks that the pre-conditions necessary for this purpose are being met.
Duty to maintain data secrecy	All persons working for the contractor's customers, including vicarious agents, are required by the contractor to give an undertaking that they will comply with applicable data protection duties under art. 28 para. 3 sentence 2 letter b, 29, 32 para. 4 GDPR.
Awareness training	All persons working for the contractor's customers are regularly trained and made aware of data protection issues by external data protection officers, generally on an annual basis.
Periodic checks on compliance with these TOM	Regular monitoring, assessment and evaluation of the effectiveness of the technical and organisational measures to be taken is carried out by an independent organisation, eg. the external data protection officer.

4.2. Incident Response Management

Aim: To guarantee that personal data processed under contract can only be processed in accordance with the customer's instructions

Situation:

Within the framework of his TISAX measures (see introductory comments to this document), the contractor has drawn up a concept for handling security incidents ("Security concept - handling security incidents"), which will be sent on request. In essence, the concept includes the following procedure:

Every message to the contractor's support service is assessed with regard to data security. Depending on the result of the assessment, the data controllers highlight the incident and derive suitable measures to ensure that the customer can fulfil his data obligations arising from arts. 33 and 34 GDPR.

4.3. Privacy by design, privacy by default (art. 25 para. 2 GDPR)

Aim: To guarantee that personal data processed under contract can only be processed in accordance with the customer's instructions

Situation:

The use of the whole platform is voluntary, inputting any data category by your users is optional. Apart from a verification of usage authorisation for each user account, in the view of the contractor users are free to enter any data, including false or pseudonymous data, without any disadvantages being thereby incurred by the data subjects. There is therefore no requirement for further action on the part of the contractor as the party offering the platform.

4.4. Contract monitoring

Aim: To guarantee that personal data processed under contract can only be processed in accordance with the customer's instructions

Measures taken:

Area	Situation
Archiving instructions	Depending on the type of instruction, the ticket system used by the contractor or the archiving of email correspondence with the customer provide transparency in order to demonstrate that data are only entered or altered/erased in accordance with the contract.
Access log	All read and write accesses to data are logged to the specific user.
Archiving of emails making reference to instructions	Emails making reference to instructions are backed up for the purpose of retrospectively tracking and providing evidence of instructions.
Regular inspection of sub-contracted processing staff	The processing staff sub-contracted by the contractor are inspected twice-yearly for compliance with the technical and organisational measures to be taken by them.

Annex 2

Sub-contracted processing staff ("SPS")

The following companies provide (part-) services within the framework of the services which are the object of the contract provided by the contractor for the customer.

Name, address	**(Part)-services**	**Data processing by SPSs**	**Processing site(s)**	**Relevant certification**	**Guarantees under art. 44 et seq.**
Heinlein Support GmbH Schwedter Straße 8/9B 10119 Berlin Germany	Provision of premises and technical prerequisites for the LXT server operation	Erasure of data within the context of the destruction of defective data supports.	EU: Berlin, Germany	Its UAV IPB GmbH is certified to ISO 27001.	[none required]
Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, 1855 Luxemburg, Luxemburg	Operation of server infrastructure for LXT installation(s) used	All data processing within the context of the contractor's provision of service.	EU: Frankfurt, Germany	ISO 27001, ISO 27017, ISO 27018	EU standard contract clauses