datenschutz nord

Version 13/11/2023

General Terms and Conditions DSN port (GTC DSN port)

of

datenschutz nord GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

(Licensor)

Preamble

The licensor provides the licensee with the software solution DSN port, including the agreed-upon modules (hereinafter also referred to as "Software"). The licensor makes an offer to the licensee in this regard. If the licensee accepts the offer, a license agreement is concluded under the following conditions. The licensor is the author and owner of all usage rights to the Software.

§ 1 Subject of the contract

(1) The licensor grants the use of the software in the respective current version and to the extent offered as a software-as-a-service-solution (SaaS). The licensor reserves the right to provide further functionalities and performance improvements in the course of the contract period.

(2) The subject of this contract is the granting of usage rights to the software to the extent offered. In this context, "usage" means enabling access to the software installed in the licensor's data center with the availability defined in Section 3, including user support (support) regarding system access. The provision of the software on physical media or download options and addressing data protection-related issues are not part of the usage.

(3) In addition to these General Terms and Conditions the parties also enter into the supplementary agreement **“Data Processing Agreement (DPA)”** as outlined in the **Addendum**.

(4) Installation and configuration services are not covered by this agreement. Any workshops or training courses that provide the licence holder with knowledge on the proper use of DSN train shall be agreed upon separately.

§ 2 Rights of use

(1) The licensor grants the licensee a paid, time-limited, non-exclusive right to use the software (license) for the duration of the contract. The license authorizes

the use of the software within the scope of normal use. The license does not extend to other types of usage.

(2) The licensee receives an agreed-upon number of access rights for specified users. The use of these access rights by other users within the same company requires consultation with the licensor.

(3) The licensee is not allowed to sublicense the software in any other way, publicly reproduce or make it accessible, or provide it to third parties, whether for a fee or free of charge. DSN train must not be made utilizable for their own or third-party purposes through reverse engineering, dismantling, testing, or any other actions.

(4) The use of the software requires a standard and up-to-date HTML5-compatible browser.

§ 3 Availability

(1) With the exception of planned downtime due to necessary updates and similar changes at the instigation of the licensor, the licensor predicts an average annual availability upwards of 95%.

(2) Major updates and similar performance improvements or bug fixes that limit the availability of the software for a defined period of time will be communicated to the licence holder in due time.

§ 4 Contract term, termination

(1) Unless otherwise agreed, the contract is concluded for a period of 12 months. If the contract is not terminated in writing at the latest three months before its expiration, it will automatically renew for an additional 12 months.

(2) Termination for good cause remains unaffected.

§ 5 Support and Warrant

(1) The licensor provides support during regular business hours to maintain the agreed quality of the software during the contract period. No further support is provided.

(2) The licensor warrants the agreed upon quality of the software and that the licensee may use the software without infringing the rights of third parties. The warranty does not apply to defects that are rooted in the software or hardware environment of the licensee.

(3) The licensor will correct errors in the software that significantly impair its intended use. Error correction will be carried out by the licensor, depending on the significance of the error, through the provision of an improved software version.

(4) The licensor guarantees continued maintenance and regular update of the software so that it can continue to be used as intended in the future.

§ 6 Liability

(1) The licensor shall be liable for damages caused by intent or gross negligence as well as for the culpable breach of essential contractual obligations in accordance with the provisions of the German Product Liability Act (ProdHaftG), insofar as this breach was caused in a manner that jeopardises the achievement of the purpose of the contract.

(2) In the event of a breach of a cardinal obligation (an obligation that is essential for achieving the purpose of the contract), the liability of the licensor shall be limited to the damage that is foreseeable and typical according to the nature of the transaction in question and the occurrence of which the licensor could typically expect based on the circumstances known to it at that time. Further liability of the licensor does not exist.

(3) The aforementioned limitation of liability also applies to the personal liability of the licensor's employees, representatives and bodies.

§ 7 Final provisions

(1) The licensee agrees that the licensor may use their company name and company logo for reference purposes. The licensee can withdraw their consent for the use of their company name and logo at any time.

(2) Should one of the present provisions be invalid, this shall not affect the validity of the remaining provisions.

(3) In this case, the invalid provision shall be replaced by the statutory provision which, according to the assumed intention of the parties, comes closest to the economic purpose of the invalid provision.

(4) German law shall apply. The place of jurisdiction is Bremen.

DocuSigned by:
Stephan Roth
A9293E1CC5E74C0...
Prokurist

Addendum: Data Processing Agreement (DPA)

between

the licensee

– hereinafter referred to as the "**Data Controller**" or "**Controller**" –

and

datenschutz nord GmbH, Konsul-Smidt-Straße 88, 28217 Bremen

– hereinafter referred to as "**Processor**" –

and collectively referred to as the "**Contracting Parties**" – the following is agreed:

Preamble

The following provisions apply to the software-as-a-service products and services of the Processor specified in **Annex 1**. In order to provide the products and services specified in Annex 1, the Processor shall carry out the data processing activities listed therein.

Since access to personal data cannot be ruled out in the course of providing services by the Processor, the contracting parties shall conclude the following provisions in accordance with Article 28 of the GDPR.

§ 1 Subject matter, nature, purpose and duration of commissioned processing

Details of the subject matter, nature, purpose and duration of the processing as well as the categories of data processed and the data subjects are described in more detail in **Annex 1**.

§ 2 Instructions of the Controller

(1) The Processor shall process personal data only for the purposes listed in **Annex 1** or only on the basis of documented instructions from the Controller, unless such processing is required under Union law or the law of a Member State to which the Processer is subject. In such a case, the Processor shall notify the Controller of those legal requirements prior to the processing, unless the law in question prohibits such notification.

(2) The Processor shall inform the Controller without undue delay if it considers an instruction to be in breach of applicable Union or Member State data protection rules.

(3) Processing of personal data by the Processor for other purposes, in particular for its own purposes, is not permitted.

§ 3 Technical and organisational measures

(1) The Processor shall at a minimum have the technical and organisational measures listed in **Annex 3** in place, to ensure the security of personal data. The measures shall ensure a level of protection appropriate to the risk. When assessing the adequate level of protection, the Parties shall take into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing and the categories of data (in particular pursuant to Article 9(1) or Article 10 of the GDPR) as well as the different probabilities of occurrence and the severity of the risk for the data subjects.

(2) The technical and organisational measures listed in **Annex 3** are subject to technical progress and further development. The measures in place shall be updated by the Processor if the level of security, specified at the time of the conclusion of the contract, can no longer be guaranteed. Any adaptations must at a minimum achieve the level of protection of the previous measures.

§ 4 Obligations of the Processor

(1) The Processor confirms that it is aware of the relevant data protection regulations. Within its area of responsibility, the processor organises its internal operations to meet the specific requirements of data protection.

(2) The Processor shall only grant its personnel access to Personal Data to the extent strictly necessary for the performance, management and monitoring of the Contract. The Processor shall ensure that the persons authorised to process Personal Data are bound by a duty of confidentiality or are subject to an appropriate legal obligation of secrecy.

(3) To the extent required by law, the Processor shall appoint a Data Protection Officer and provide their contact details in **Annex 1.**

(4) The Processor shall perform the commissioned processing in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. The processing of personal data in a third country always requires the prior, documented consent of the Controller and may only take place if the specific legal requirements of the GDPR are met.

§ 5 Support obligations of the Processor

(1) Taking into account the nature of the processing and the information at its disposal, the Processor shall assist the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR.

(2) Furthermore, in view of the nature of the processing, the Processor shall, where possible, assist the Controller with appropriate technical and organisational measures to comply with its obligation to respond to requests to exercise the rights referred to in Chapter III of the GDPR.

§ 6 Authorisation to establish subcontracting relationships

(1) The Processor shall have the general authorisation of the Controller to subcontract with Processors. The Processor shall inform the Controller in advance, in text form, of all intended sub-Processor engagements so that the Controller may object prior to the engagement. The use of the sub-Processors listed in **Annex 2** at the time of signing the contract shall be deemed to be approved, provided that the requirements set out in Article 6(2) of this contract are implemented.

(2) Access to personal data by the sub-Processor may only take place if the Processor ensures by means of a written contract, which may also be concluded in an electronic format, with the sub-Processor that the rules agreed in this contract also apply to the sub-Processor.

(3) The Processor shall notify the Controller of any breach of contractual obligations by the Sub-Processor.

(4) The Processor shall ensure compliance with the provisions of Article 44 et seq. of the GDPR in the event of a subcontract involving a transfer of personal data within the meaning of Chapter V of the GDPR - if necessary - providing appropriate safeguards in accordance with Article 46 GDPR.

(5) The Processor undertakes, in cases where it uses a sub-Processor and where the processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, to conclude standard contractual clauses with the sub-Processor pursuant to Article 46 of the GDPR, provided that the conditions for the application of such standard contractual clauses are met

§ 7 Control rights of the Controller

(1) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in this Contract or directly resulting from the GDPR. At the request of the Controller, the Processor shall also allow and contribute to the audit of the processing activities covered by this Contract at appropriate intervals or where there are indications of non-compliance. When deciding on a review or audit, the Controller may take into account relevant certifications within the meaning of Article 28(5) GDPR of the Processor.

(2) The Controller may conduct the audit itself or engage an independent auditor. The audits may also include inspections of the premises or physical facilities of the Processor, where appropriate and shall be carried out with reasonable advance notice and in compliance with the Processor's business and trade secrets and - if possible - without disrupting the business operations.

(3) The Parties shall make the information referred to in this Agreement, including the results of audits, available to the competent supervisory authorities upon request.

§ 8 Data Breaches to be reported

(1) The Processor shall inform the Controller without undue delay of any disruptions to the operational process that pose a risk to the Controller's data and of any data protection breaches in connection with the Controller's data that become known. The same shall apply if the Processor determines that the security measures taken by it do not meet the legal requirements.

(2) The Processor is aware that the Controller is obliged to comprehensively document all breaches of the protection of personal data and, if necessary, to report them to the supervisory authorities or the data subject. If such breaches occur in the sphere of the Processor, the Processor shall inform the Controller without delay and shall provide the Controller with at least the following information:

(1) description of the nature of the breach, including, where possible, the categories and approximate number of individuals and records affected,

(2) name and contact details of contact persons for further information,

(3) description of the likely consequences of the breach, and

(4) description of the measures taken or proposed to remedy the breach or mitigate the resulting adverse effects.

§ 9 Termination of the order

(1) Upon termination of the commissioned processing, the Processor shall either delete or return all personal data at the discretion of the Controller, unless there is a legal obligation to store the personal data. This also applies to any backup copies in accordance with the technical and organisational measures taken.

(2) The Controller may terminate the contract without notice if the Processor commits a serious breach of the provisions of this contract or of data protection law and the Controller cannot reasonably be expected to continue processing the order until the expiry of the notice period or until the agreed termination of the contract.

(3) The Processor may terminate the contractual relationship without observing a notice period if the Controller insists on the implementation of its instructions, despite these instructions contravening applicable legal requirements or breaching this contract, and the data processor has informed the data controller accordingly.

§ 10 Accession to the contract

Additional parties may accede to this contract as Controllers or Processors at any time with the consent of all contracting parties by means of a declaration of accession. In addition to the declaration of accession, **Annexes 1 to 3** shall be completed as necessary. As of the date of accession, the acceding parties shall be deemed to be contracting parties to this contract with the rights and obligations existing according to their designation.

§ 11 Final provisions

(1) If the property of the Controller in the possession of the Processor is endangered by measures of third parties (e.g. by seizure or confiscation), by insolvency proceedings or by other events, the Processor must inform the Controller immediately. A right of retention is excluded with regard to data carriers and data files of the Controller.

(2) The grounds for the contract, amendments to the contract and ancillary agreements must be in writing, which may also be in an electronic format.

(3) In the event of any conflict between these contractual clauses and the provisions of any related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

(4) Should specific parts of this contract be invalid, this shall not affect the validity of the rest of the contract.

DocuSigned by:
Stephan Rothe
A9293E1CC5E74C0...

Prokurist

Annex 1

Software-as-a-Service products and services of the order Processor

Software-as-a-Service products	**DSN port** with the modules • **privacy** – The Data Protection Management System • **datenschutzBR** – The Data Protection Management System for works councils • **learning** – The Learning Management System (LMS) Hereafter collectively "software" or "applications".
Services	• Provision • Hosting • Maintenance, service and support

Subject matter, nature, purpose and duration of the processing, categories of personal data and persons concerned

Subject of the processing	Provision of software (software-as-a-service) including hosting as well as maintenance, service and support services
Nature and purpose of the processing	Provision of software (software-as-a-service) including hosting as well as maintenance, service and support services
Category of personal data	• User data (e.g. surname, first name, business e-mail address) • Service provider or contractual data (e.g. name, business contact details of service providers or contractual partners of the responsible party) • Data recorded for specific reasons (e.g. information on data breaches, data subject enquiries, existing contractual relationships) • Log files, IDs and IP addresses of the users In the case of the module **learning,** moreover: • Training participant data (e.g. surname, first name, title, business email address, learning progress).

Categories of data subjects	• Employees of the Controller • Service provider/contract partner/contact person of the Controller • If applicable, data subjects or other third parties in the case of documentation of data subject enquiries or data breaches.
Duration of the processing	corresponds to the license duration

Contact details of the data protection officer

Data Protection Officer of the Processor	Florian Wallrapp E-mail: dsb@dsn-group.de

Annex 2

List of appointed subcontractors and processing sites

SUBCONTRACTOR	PROCESSING STATUS - LOCATION	DESCRIPTION OF THE PROCESSING
PLUTEX GmbH, Hermann-Ritter-Str. 110, 28197 Bremen	Bremen	Provision of servers in an ISO/IEC 27001 certified data center in Bremen

Annex 3

Technical and organisational measures according to Art. 32 DSGVO

This Annex specifies the technical and organisational measures taken in accordance with Article 32 (1) of the GDPR to ensure the security of the processing of personal data. The Processor shall take the following measures, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons.

1. Measures for pseudonymisation and encryption

Personal data is always pseudonymised, insofar as this is possible according to the purpose of use and does not require a disproportionate effort in relation to the intended protective purpose. If IP addresses are required for the delivery of content, these are generally not stored or anonymised. In order to be able to recognise, limit and eliminate attacks on our applications, we store IP addresses in an unabbreviated form by way of exception, but only for strictly specific purposes for a maximum of seven days.

Hard disks of the end devices with which personal data of the data Controller are processed are encrypted.

In order to ensure that data cannot be read, copied or changed by unauthorised persons during electronic transmission or transport, state-of-the-art encryption protocols are used (e.g. https/TLS 1.2 or 1.3). Administrative access to the server systems is only possible from the company network of the Processor.

Passwords are not stored in plain text in the applications, but only in hashed form.

2. Measures to ensure confidentiality

2.1. Access control measures

In order to prevent unauthorised persons from gaining access to the offices and to data processing systems on which personal data of the Controller are processed, access is secured by a mechanical locking system (key) as well as an electronic locking system (transponder + PIN). Even during business hours, all entrance doors are locked and can only be opened from the inside using a handle or from the outside using a suitable key/transponder.

The transponders and keys for the locking system are issued on a person-specific basis. The issuing and return of transponders and keys are logged. In addition, successful accesses and unsuccessful access attempts are logged in the locking system

There is no visitor traffic in the office building in which the data processing systems are located. If persons from outside the company are granted access to the office building, they will be met at the entrance and may only be in the building in the company of an employee.

Outside business hours, the offices are monitored by a burglar alarm system (alarm activation by a security service). Unauthorised access attempts will trigger the burglar alarm system. In the event of an alarm, a commissioned security service and the employees of the Processor responsible for the intrusion alarm system shall be informed.

The Processor operates its own server room on the office premises described in more detail above. This room has no windows and is additionally secured with a mechanical lock. Access to the server room is limited to a few authorised persons. The servers operated by the company serve exclusively as backup servers.

If data is processed in the externally used data centre of the hosting service provider named in **Annex 2**, the hosting service provider shall take suitable measures to prevent unauthorised persons from accessing the data processing facilities. These include, for example, the operation of an alarm system, the use of smart card/transponder locking systems with PIN code (two-factor authentication), video surveillance of the access points and personal control measures.

2.2. Access control measures

To prevent data processing systems from being used by unauthorised persons, they can only be used after sufficient authentication.

Administrative access to the systems requires the entry of a user name and password or multi-factor authentication. The administrator passwords contain at least ten characters, consisting of upper and lower case letters as well as special characters and numbers. In addition, administrative activities on the server side can only be carried out from the corporate network of the Processor. In addition, so-called security tokens/smartcards and PINs are used for administrative access.

Employees of the Processor are also instructed to lock their clients when leaving the workplace and to activate the automatic screen lock when inactive. Furthermore, there is a limitation of unsuccessful login attempts and a separate authentication for remote access.

When logging on to the client systems of the Processor, the user name and password are requested. The passwords used for hard disk encryption shall comprise at least 30 characters as well as lower and upper case letters, special characters and numbers. Otherwise, the passwords used must be at least eight characters long and contain lower and upper case letters, special characters and numbers.

Users of the applications authenticate themselves via multi-factor authentication. In addition to requesting a user name and password, one of the following three additional factors are used for authentication: a one-time password procedure, a browser fingerprinting procedure or an IP whitelisting procedure.

The system ensures that sufficiently complex passwords consisting of at least ten characters, a lower case letter, an upper case letter, a special character and a number are used for authentication.

In addition, the Processor has taken measures to detect a possible compromise of passwords. To this end, users of the software receive a message about their last login after each login, for example.

In the context of the LMS module 'learning,' the following applies regarding authentication for access to the training room:

The persons participating in the training can authenticate themselves to the system by means of a so-called deeplink, QR code, OpenID login as well as by means of user name and password.

In the case of the deeplink login, the training participants receive their access data by e-mail. The security settings of the e-mail systems used offer additional protection. In addition, the application ensures that deep links cannot be used more than once. The possibility of registering via QR login code is, however, limited in time.

2.3. Access control measures

In order to ensure that those authorised to use a data processing system can only access data assigned to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage, access rights are assigned strictly according to the need-to-know principle on the basis of authorisation concepts.

2.4. Measures for transfer control

To ensure that personal data cannot be read, copied, changed or removed without authorisation during electronic transmission or during transport or storage on data carriers, the applications can only be accessed via sufficiently secure encrypted connections, e.g. using https/TLS 1.2 and TLS 1.3 encryption.

If temporary access to individual web forms is granted by means of so-called deep links, these are secured by a sufficiently long ID that cannot be guessed and a password.

2.5. Measures to implement the separation requirement

Logical data separation (client separation) and authorisation concepts on the application side ensure that the data of the Controller is processed separately from the data of other Controller.

2.6. Disposal of paper documents, mobile data carriers and terminal devices

Shredders are available for the disposal of paper documents with personal data that are no longer needed, and their use is instructed.

Data carriers or end devices that are no longer needed are cleaned by an external service provider before they are disposed of in accordance with data protection regulations.

3. Measures to ensure integrity (input control)

In order to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed, the entry, change and removal of data is logged by the system. By means of an internal logging system, it can be determined retrospectively at which points data was entered, changed or deleted at application level.

Access to this log data takes place - in accordance with the authorisation concept - using individual user names and passwords as well as key-based authentication.

4. Measures to ensure availability

In order to ensure that Personal Data is protected against accidental destruction or loss, the Processor shall take the following measures:

- Processor systems on which personal data are processed are secured by a firewall; incoming and outgoing e-mails are automatically checked for malware.
- Security-relevant software updates are installed immediately.
- The applications' databases are fully backed up locally several times a day and geo-redundantly once a day.
- The data centre of the hosting service provider named in **Annex 2**, which is used externally by the Processor, has an uninterruptible power supply that prevents the data stock from being damaged in the event of a sudden power failure. The data centre is also air-conditioned and has appropriate fire protection measures.

5. Measures for the rapid restoration of availability

According to existing recovery plans, in the event of a single system failure, the applications are automatically moved to other servers in the same hosting environment. In the event of a large cluster failure, a degraded version of the services can be manually provisioned on a separate cluster in the same data centre. In the event of a complete data centre failure, the service can be fully restored using a documented procedure once a functioning Kubernetes cluster is available.

Backups are stored close to the production hardware for faster recovery. Backups are mirrored every night for redundancy. Copies are kept in the Processor's building. Another, fully encrypted copy is stored for redundancy in a data centre operated by an external service provider (Ionos SE, based in Germany).

The hosting service provider commissioned by the Processor and specified in **Annex 2** shall have its own backup and recovery concepts and contingency plans.

6. Measures to ensure the resilience of systems and services

Resilient systems (hardware and software) are used that can withstand the expected demands in terms of storage, access and performance capacities. The same applies with regard to the hosting service provider described in more detail in **Annex 2**.

7. Other technical and organisational measures

7.1. Order control

Insofar as further Processors support the Processor in the processing of personal data of the Controller, processing contracts shall be concluded in accordance with Article 28 of the GDPR. In addition, the Processor shall ensure that sub-processorshave appropriate technical and organisational measures in place, in accordance with Article 32 of the GDPR.

7.2. Information, awareness and training management

Employees of the Processor are obliged to comply with the data protection principles when they are hired and are sensitised to the topics of data protection and data security in regular training sessions.

Employees of the Processor who are involved in processing shall closely follow the reports on security vulnerabilities in relation to the software components used.

7.3. Data protection management and IT security management including procedures for regular review, assessment and evaluations

The Processor has appointed a Data Protection Officer who performs the tasks described in Article 39 of the GDPR and has the necessary qualifications and expertise in the field of data protection law and practice.

In addition, the Processor has appointed an Information Security Officer who supports the Processor as a central coordination point in the design of information security and the implementation and control of corresponding business processes.

Measures taken by the Processor to maintain data protection and information security shall be reviewed regularly. In particular, the technical and organisational measures documented in this Annex shall be reviewed and, if necessary, adapted to the state of the art.

Anhang 3

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Dieser Anhang konkretisiert die nach Art. 32 Abs. 1 DSGVO getroffenen technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten. Der Auftragsverarbeiter trifft nachfolgende Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

8. Maßnahmen zur Pseudonymisierung und Verschlüsselung

Personenbezogene Daten werden grundsätzlich pseudonymisiert, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Sofern zur Auslieferung von Inhalten IP-Adressen erforderlich sind, werden diese grundsätzlich nicht gespeichert bzw. anonymisiert. Um Angriffe auf unsere Anwendungen erkennen, eingrenzen und beseitigen zu können, speichern wir IP-Adressen ausnahmsweise ungekürzt, jedoch lediglich streng zweckgebunden für die Dauer von maximal sieben Tagen.

Festplatten der Endgeräte, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden, werden verschlüsselt.

Um zu gewährleisten, dass Daten auch bei der elektronischen Übertragung bzw. während des Transports nicht von Unbefugten gelesen, kopiert oder verändert werden können, werden modernste Verschlüsselungsprotokolle, die dem Stand der Technik entsprechen, eingesetzt (bspw. https/TLS 1.2 bzw. 1.3). Administrative Zugriffe auf die Serversysteme sind zudem nur aus dem Firmennetzwerk des Auftragsverarbeiters möglich.

Passwörter werden in den Anwendungen nicht im Klartext gespeichert, sondern ausschließlich in gehashter Form.

9. Maßnahmen zur Gewährung der Vertraulichkeit

9.1. Maßnahmen zur Zutrittskontrolle

Um Unbefugten den Zutritt zu den Büroräumen sowie zu Datenverarbeitungsanlagen zu verwehren, auf denen personenbezogene Daten des Verantwortlichen verarbeitet werden, wird der Zutritt sowohl über ein mechanisches Schließsystem (Schlüssel) als auch ein elektronisches Schließsystem (Transponder + PIN) gesichert. Auch während der Geschäftszeiten sind alle Eingangstüren verschlossen und können nur per Klinke von innen oder mit einem passenden Schlüssel/Transponder von außen geöffnet werden.

Die Transponder und Schlüssel für das Schließsystem werden personenbezogen vergeben. Transponderausgabe und Schlüsselausgabe sowie -rückgabe werden protokolliert. Daneben werden systemseitig erfolgreiche Zutritte sowie erfolglose Zutrittsversuche im Schließsystem protokolliert.

In dem Bürogebäude, in dem sich die Datenverarbeitungsanlagen befinden, herrscht kein Besucherverkehr. Sofern ausnahmsweise betriebsfremden Personen Zutritt zum Bürogebäude gewährt wird, werden diese am Eingang abgeholt und dürfen sich im Gebäude nur in Begleitung eines/einer Beschäftigten aufhalten.

Außerhalb der Geschäftszeiten werden die Büroräume mit einer Einbruchmeldeanlage überwacht (Alarmaufschaltung bei einem Sicherheitsdienst). Unberechtigte Zutrittsversuche haben das Auslösen der Einbruchmeldeanlage zur Folge. Im Falle eines Alarms werden ein beauftragter Sicherheitsdienst und die für die Einbruchmeldeanlage zuständigen Mitarbeitenden des Auftragsverarbeiters informiert.

Der Auftragsverarbeiter betreibt einen eigenen Serverraum in den vorstehend näher beschriebenen Büroräumen. Dieser ist fensterlos und zusätzlich mit einem mechanischen Schloss abgesichert. Der Zutritt zum Serverraum ist auf wenige zutrittsberechtigte Personen beschränkt. Die eigenbetriebenen Server dienen ausschließlich als Backup-Server.

Soweit Daten in dem extern genutzten Rechenzentrum des im **Anhang 2** genannten Hosting-Dienstleisters verarbeitet werden, trifft dieser geeignete Maßnahmen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen zu hindern. Hierzu zählen bspw. der Betrieb einer Alarmanlage, der Einsatz von Chipkarten-/Transponder-Schließsysteme mit PIN-Code (Zwei-Faktor-Authentifizierung), die Videoüberwachung der Zugänge sowie Personenkontrollmaßnahmen.

9.2. Maßnahmen zur Zugangskontrolle

Um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, ist die Nutzung dieser erst nach hinreichender Authentifizierung möglich.

Dabei setzen administrative Zugänge zu den Systemen die Eingabe eines Nutzernamens und eines Passworts bzw. eine Multi-Faktor-Authentifizierung voraus. Die Administratoren-Passwörter enthalten mindestens zehn Zeichen, bestehend aus großen und kleinen Buchstaben sowie Sonderzeichen und Ziffern. Zudem können administrative Tätigkeiten serverseitig nur aus dem Unternehmensnetz des Auftragsverarbeiters durchgeführt werden. Zusätzlich werden für administrative Zugriffe sog. Security-Token/Smartcard nebst PIN verwendet.

Mitarbeitende des Auftragsverarbeiter sind zudem angewiesen, ihre Clients beim Verlassen des Arbeitsplatzes zu sperren und die automatische Bildschirmsperre bei Inaktivität zu aktivieren. Ferner findet eine Begrenzung der erfolglosen Anmeldeversuche sowie eine gesonderte Authentifizierung bei Fernzugängen statt.

Bei der Anmeldung an den Client-Systemen des Auftragsverarbeiters werden Benutzername und Passwort abgefragt. Die verwendeten Passwörter umfassen in Bezug auf die Festplattenverschlüsselung mindestens 30 Zeichen sowie Klein- und Großbuchstaben, Sonderzeichen und Ziffern. Im Übrigen müssen die verwendeten Passwörter mindestens acht Zeichen umfassen sowie Klein- und Großbuchstaben, Sonderzeichen und Ziffern enthalten.

Nutzende der Anwendungen authentifizieren sich über eine Multi-Faktor-Authentifizierung. Neben Abfrage von Benutzernamen und Passwort wird einer der folgenden drei zusätzlichen Faktoren zur Authentifizierung genutzt: ein One-Time-Passwort-
Verfahren, ein Browser-Fingerprinting-Verfahren oder ein IP-Whitelisting-Verfahren.

Systemseitig wird sichergestellt, dass hinreichend komplexe Passwörter, bestehend aus mindestens zehn Zeichen, einem Kleinbuchstaben, einem Großbuchstaben, einem Sonderzeichen und einer Zahl, für die Authentifizierung genutzt werden.

Zudem wurden seitens des Auftragsverarbeiters Maßnahmen ergriffen, um eine mögliche Kompromittierung von Passwörtern zu erkennen. Hierfür erhalten Nutzende der Software bspw. nach jeder Anmeldung einen Hinweis zu ihrem letzten Login.

In Bezug auf die Authentifizierung gegenüber dem im Rahmen des LMS-Moduls learning zur Verfügung stehenden Schulungsraumes gilt folgendes:

Die an der Schulung teilnehmenden Personen können sich gegenüber dem System mittels sog. Deeplink-, QR-Code, OpenID-Login sowie mittels Benutzername und Passwort authentifizieren.

Im Falle des Deeplink-Logins erhalten die Schulungsteilnehmenden ihre Zugangsdaten per E-Mail. Hierdurch bieten die Sicherheitseinstellungen der verwendeten E-Mail-Systeme zusätzlichen Schutz. Zudem wird anwendungsseitig sichergestellt, dass Deeplinks nicht mehrfach verwendet werden können. Die Möglichkeit der Anmeldung per QR-Login-Code ist indes zeitlich begrenzt.

9.3. Maßnahmen zur Zugriffskontrolle

Um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, werden Zugriffsrechte streng nach dem Need-to-Know-Prinzip auf der Grundlage von Berechtigungskonzepten vergeben.

9.4. Maßnahmen zur Weitergabekontrolle

Um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden, können die Anwendungen nur über hinreichend sicher verschlüsselte Verbindungen angesteuert werden, z. B.
mittels https-/TLS 1.2- und TLS 1.3-Verschlüsselung.

Sofern temporäre Zugriffe auf einzelne Web-Formulare mittels sog. Deep-Links gewährt werden, werden diese über eine ausreichend lange ID, die nicht erraten werden kann, sowie ein Passwort abgesichert.

9.5. Maßnahmen zur Umsetzung des Trennungsgebots

Durch eine logische Datentrennung (Mandantentrennung) und anwendungsseitige Berechtigungskonzepte ist sichergestellt, dass die Daten des Verantwortlichen getrennt von den Daten anderer Verantwortlicher verarbeitet werden.

9.6. Entsorgung von Papierunterlagen, mobilen Datenträgern und Endgeräten

Für die Entsorgung nicht mehr benötigter Papierunterlagen mit personenbezogenen Daten stehen Schredder zur Verfügung, deren Nutzung angewiesen ist.

Nicht mehr benötigte Datenträger oder Endgeräte werden vor der datenschutzkonformen Entsorgung durch einen externen Dienstleister bereinigt.

10. Maßnahmen zur Gewährung der Integrität (Eingabekontrolle)

Um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind, wird die Eingabe, Veränderung und Entfernung von Daten systemseitig protokolliert. Durch ein internes Protokollsystem kann nachträglich festgestellt werden, an welchen Stellen Daten auf Anwendungsebene eingegeben, verändert oder gelöscht wurden.

Der Zugriff auf diese Protokolldaten erfolgt – gemäß dem Berechtigungskonzept – unter Verwendung von individuellen Benutzernamen und Passwörtern sowie key-basierter Authentifizierung.

11. Maßnahmen zur Gewährleistung der Verfügbarkeit

Um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, trifft der Auftragsverarbeiter nachfolgende Maßnahmen:

- Systeme des Auftragsverarbeiters, auf denen personenbezogene Daten verarbeitet werden, werden durch eine Firewall abgesichert; ein- und ausgehende E-Mails werden automatisch auf Malware geprüft.
- Sicherheitsrelevante Software-Updates werden unverzüglich installiert.
- Die Datenbestände der Anwendungen werden mehrfach täglich lokal und einmal täglich georedundant voll gesichert.
- Das vom Auftragsverarbeiter extern genutzte Rechenzentrum des im **Anhang 2** genannten Hosting-Dienstleisters verfügt über eine unterbrechungsfreie Stromversorgung, die verhindert, dass der Datenbestand bei einem plötzlichen Stromausfall Schaden nehmen kann. Das Rechenzentrum ist zudem klimatisiert und verfügt über angemessene Brandschutzmaßnahmen.

12. Maßnahmen zur raschen Wiederherstellbarkeit der Verfügbarkeit

Entsprechend vorhandener Wiederherstellungspläne werden die Anwendungen im Falle eines einzelnen Systemausfalls automatisch auf andere Server in derselben Hosting-Umgebung umgestellt. Im Falle eines Ausfalls eines großen Clusters kann manuell eine degradierte Version der Dienste auf einem separaten Cluster im selben

Rechenzentrum bereitgestellt werden. Im Falle eines vollständigen Ausfalls des Rechenzentrums kann der Dienst anhand eines dokumentierten Verfahrens vollständig wiederhergestellt werden, sobald ein funktionierendes Kubernetes-Cluster vorhanden ist.

Backups werden in der Nähe der Produktionshardware gespeichert, um eine schnellere Wiederherstellung zu ermöglichen. Die Sicherungen werden jede Nacht aus Redundanzgründen gespiegelt. Kopien werden im Gebäude des Auftragsverarbeiters aufbewahrt. Eine weitere, vollständig verschlüsselte Kopie wird zur Redundanz in einem
Rechenzentrum gespeichert, das von einem externen Dienstleister (Ionos SE mit Sitz in Deutschland) betrieben wird.

Der vom Auftragsverarbeiter beauftragte, im **Anhang 2** näher genannte, Hosting-Dienstleister verfügt über eigene Backup- und Recovery-Konzepte sowie Notfallpläne.

13. Maßnahmen zur Gewährleistung der Belastbarkeit von Systemen und Diensten

Es werden widerstandsfähige Systeme (Hard- und Software) eingesetzt, die im Hinblick auf die Speicher-, Zugriffs- und Leistungskapazitäten den zu erwartenden Beanspruchungen standhalten. Entsprechendes gilt im Hinblick auf den im **Anhang 2** näher bezeichneten Hosting-Dienstleister.

14. Sonstige technische und organisatorische Maßnahmen

14.1. Auftragskontrolle

Soweit weitere Auftragsverarbeiter den Auftragsverarbeiter bei der Verarbeitung personenbezogener Daten des Verantwortlichen unterstützen, werden mit diesen Auftragsverarbeitungsverträge nach Art. 28 DSGVO geschlossen. Zudem stellt der Auftragsverarbeiter sicher, dass auch diese angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO treffen.

14.2. Informations-, Sensibilisierungs- und Schulungsmanagement

Mitarbeitende des Auftragsverarbeiters werden bei Einstellung zur Einhaltung der Datenschutzgrundsätze verpflichtet und in regelmäßig stattfindenden Schulungen in den Themenbereichen Datenschutz und Datensicherheit sensibilisiert.

An der Auftragsverarbeitung beteiligte Mitarbeitende des Auftragsverarbeiters verfolgen zudem aufmerksam die Berichte über Sicherheitslücken in Bezug auf die verwendeten Softwarekomponenten.

14.3. Datenschutzmanagement und IT-Sicherheitsmanagement einschließlich Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierungen

Der Auftragsverarbeiter hat einen betrieblichen Datenschutzbeauftragten bestellt, der die in Art. 39 DSGVO näher beschriebenen Aufgaben wahrnimmt und die hierfür

erforderlichen Qualifikationen und Fachkenntnisse auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis mitbringt.

Zudem hat der Auftragsverarbeiter einen/eine Informationssicherheitsbeauftragte/n bestellt, der/die den Auftragsverarbeiter als zentrale Koordinationsstelle bei der Gestaltung der Informationssicherheit sowie der Umsetzung und Kontrolle entsprechender Geschäftsprozesse unterstützt.

Vom Auftragsverarbeiter getroffene Maßnahmen zum Erhalt des Datenschutzes und der Informationssicherheit werden regelmäßig überprüft. Dabei werden insbesondere auch die in dieser Anlage dokumentierten technischen und organisatorischen Maßnahmen überprüft und im Bedarfsfall dem Stand der Technik angepasst.