datenschutz nord

Version vom 13.11.2023

Allgemeine Lizenzbedingungen DSN port (ALB DSN port)

der

datenschutz nord GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

(Lizenzgeber)

Präambel

Der Lizenzgeber stellt dem Lizenznehmer die Softwarelösung DSN port einschließlich der jeweils vereinbarten Module zur Verfügung (nachfolgend auch „Software" genannt). Der Lizenzgeber unterbreitet dem Lizenznehmer hierzu ein Angebot. Nimmt der Lizenznehmer das Angebot an, so kommt ein Lizenzvertrag zu den nachstehenden Bedingungen zustande. Der Lizenzgeber ist Urheber und Inhaber sämtlicher Nutzungsrechte an der Software.

§ 1 Vertragsgegenstand

(1) Der Lizenzgeber gewährt die Nutzung der Software in der jeweils aktuellen Version sowie in dem angebotenen Umfang als Software-as-a-Service-Lösung (SaaS). Der Lizenzgeber behält sich vor, weitere Funktionalitäten und Leistungsverbesserungen im Laufe der Vertragsdauer zur Verfügung zu stellen.

(2) Gegenstand dieses Vertrages ist die Gewährung von Nutzungsrechten an der Software in dem angebotenen Umfang. Nutzung in diesem Zusammenhang bedeutet die Ermöglichung des Zugriffs auf die im Rechenzentrum des Lizenzgebers installierte Software mit der in § 3 definierten Verfügbarkeit einschließlich Anwenderunterstützung (Support) in Bezug auf den Zugang zum System. Die Aushändigung der Software auf Datenträger oder Downloadmöglichkeit und die Stellungnahme zu datenschutzrechtlichen Fragen sind nicht Gegenstand der Nutzung.

(3) Die Parteien schließen mit Annahme des Angebots zusätzlich zu diesen Allgemeinen Lizenzbedingungen die Zusatzvereinbarung **„Auftragsverarbeitungsvertrag (AVV)" gemäß** Addendum.

(4) Installations- und Konfigurationsleistungen sind nicht Gegenstand dieses Vertrages. Etwaige Workshops bzw. Schulungen, die dem Lizenznehmer Kenntnisse zur fachgerechten Nutzung der Software vermitteln, werden separat vereinbart.

§ 2 Nutzungsrechte

(1) Der Lizenzgeber gewährt dem Lizenznehmer ein entgeltliches, durch die Vertragsdauer zeitlich befristetes, nicht ausschließliches Recht zur Nutzung der Software (Lizenz). Die Lizenz berechtigt zur Nutzung der Software im Rahmen eines normalen Gebrauchs. Auf andere Nutzungsarten erstreckt sich die Lizenz nicht.

(2) Zur Nutzung erhält der Lizenznehmer eine zwischen den Parteien vereinbarte Anzahl von Zugriffsmöglichkeiten für dedizierte Nutzer. Eine Nutzung dieser Zugriffsmöglichkeiten durch andere Nutzer innerhalb desselben Unternehmens bedarf der Absprache mit dem Lizenzgeber.

(3) Der Lizenznehmer darf die Software nicht in sonstiger Weise unterlizensieren, sie öffentlich wiedergeben oder zugänglich machen oder aber Dritten zur Verfügung stellen, sei es entgeltlich oder unentgeltlich. Auch darf die Software nicht durch Rückbau, Testen oder sonstige Handlungen für eigene oder fremde Zwecke verwertbar gemacht werden (Reverse Engineering).

(4) Die Nutzung der Software setzt einen üblichen und aktuellen HTML5-fähigen Browser voraus.

§ 3 Verfügbarkeit

(1) Mit Ausnahme von geplanten Nicht-Verfügbarkeiten aufgrund notwendiger Updates und ähnlicher Veränderungen auf Veranlassung des Lizenzgebers, sichert der Lizenzgeber für die Software eine durchschnittliche jährliche Verfügbarkeit von 99,5 % zu.

(2) Updates und ähnliche Leistungsverbesserungen bzw. Fehlerbehebungen, die die Verfügbarkeit der Software für einen definierten Zeitraum einschränken, werden dem Lizenznehmer mit einer Vorlaufzeit von mindestens zwei Werktagen mitgeteilt.

§ 4 Vertragslaufzeit, Kündigung

(1) Sofern nichts anderes vereinbart wird, wird der Vertrag zunächst für einen Zeitraum von 12 Monaten geschlossen. Wenn der Vertrag nicht spätestens drei Monate vor Ablauf schriftlich gekündigt wird, verlängert er sich jeweils automatisch um weitere 12 Monate.

(2) Die Kündigung aus wichtigem Grund bleibt unberührt.

§ 6 Support und Gewährleistung

(1) Der Lizenzgeber leistet während der üblichen Geschäftszeiten Support für die Aufrechterhaltung der vertraglich vereinbarten Beschaffenheit der Software während der Vertragslaufzeit. Ein weitergehender Support ist nicht geschuldet.

(2) Der Lizenzgeber leistet Gewähr für die vereinbarte Beschaffenheit der Software und dafür, dass der Lizenznehmer die Software ohne Verstoß gegen Rechte Dritter nutzen kann. Die Gewährleistung ist nicht anwendbar auf Mängel, die in der Soft- bzw. Hardwareumgebung des Lizenznehmers begründet sind.

(3) Der Lizenzgeber wird Fehler der Software berichtigen, die die bestimmungsgemäße Benutzung erheblich beeinträchtigen. Die Fehlerberichtigung erfolgt durch den Lizenzgeber, je nach Stellenwert des Fehlers, durch die Bereitstellung einer verbesserten Softwareversion.

(4) Die Zukunftssicherheit der Software wird für den bestimmungsgemäßen Einsatz vertraglich zugesichert.

§ 7 Haftung

(1) Der Lizenzgeber haftet für Schäden, die durch Vorsatz oder grober Fahrlässigkeit entstanden sind, sowie für die schuldhafte Verletzung wesentlicher Vertragspflichten nach den Vorschriften des ProdHaftG, soweit diese Verletzung in einer das Erreichen des Vertragszwecks gefährdenden Weise verursacht wurde.

(2) Bei Verletzung einer Kardinalpflicht (Pflicht, die wesentlich für die Erreichung des Vertragszwecks ist) ist die Haftung des Lizenzgebers begrenzt auf den Schaden, der nach der Art des fraglichen Geschäfts vorhersehbar und typisch ist und mit dessen Entstehen der Lizenzgeber aufgrund der ihm zu jenem Zeitpunkt bekannten Umstände typischerweise rechnen musste. Eine weitergehende Haftung des Lizenzgebers besteht nicht.

(3) Die vorgenannte Haftungsbeschränkung bezieht sich auch auf die persönliche Haftung der Mitarbeiter, Vertreter und Organe des Lizenzgebers.

§ 8 Schlussbestimmungen

(1) Der Lizenznehmer erklärt sich damit einverstanden, dass der Lizenzgeber dessen Firmennamen sowie dessen Firmenlogo zu Referenzzwecken nutzen darf. Der Lizenznehmer kann sein Einverständnis in die Nutzung seines Firmennamens sowie seines Firmenlogos jederzeit widerrufen.

(2) Sollte eine der vorliegenden Regelungen unwirksam sein, berührt dies nicht die Wirksamkeit der übrigen Bestimmungen.

(3) Die unwirksame Regelung wird in diesem Fall durch die gesetzliche Regelung ersetzt, die nach dem angenommenen Willen der Parteien dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt.

(4) Es gilt deutsches Recht. Gerichtsstand ist Bremen.

DocuSigned by:
Stephan Rothe
A9293E1CC5E74C0...
Prokurist

Addendum: Auftragsverarbeitungsvertrag (AVV)

zwischen

dem Lizenznehmer

– nachfolgend **„Verantwortlicher“** genannt –

und der

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

– nachfolgend **„Auftragsverarbeiter“** genannt

und gemeinsam als **„Vertragsparteien“** bezeichnet – wird Folgendes vereinbart:

Präambel

Nachfolgende Regelungen gelten für die im **Anhang 1** näher genannten Software-as-a-Service-Produkte und -Dienstleistungen des Auftragsverarbeiters. Zur Bereitstellung der im **Anhang 1** näher genannten Produkte und Dienstleistungen führt der Auftragsverarbeiter die dort aufgeführten Datenverarbeitungen durch.

Da im Zuge der Leistungserbringung des Auftragsverarbeiters ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, schließen die Vertragsparteien nachfolgende Regelungen nach Art. 28 DSGVO.

§ 1 Gegenstand, Art, Zweck und Dauer der Auftragsverarbeitung

Einzelheiten zum Gegenstand, zur Art, zum Zweck und zur Dauer der Verarbeitung sowie zu den Kategorien der verarbeiteten Daten und der betroffenen Personen werden im **Anhang 1** näher beschrieben.

§ 2 Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für im **Anhang 1** aufgeführte Zwecke bzw. nur aufgrund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im **Anhang 3** aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der

personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 DSGVO bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die im **Anhang 3** aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Die Maßnahmen sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im **Anhang 1** mit.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen, dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

(2) Ferner unterstützt der Auftragsverarbeiter den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und

organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte nachzukommen.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Die Inanspruchnahme der im **Anhang 2** zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrags genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten.

(3) Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(4) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Art. 44 ff. DSGVO sicher, indem – sofern erforderlich – geeignete Garantien gemäß Art. 46 DSGVO getroffen werden.

(5) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können ggf. auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters

umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von
Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie – nach Möglichkeit – ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8 Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Treten solche Verletzungen in der Sphäre des Auftragsverarbeiters auf, informiert dieser den Verantwortlichen unverzüglich und teilt diesem zumindest folgende Informationen mit:

(1) Eine Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,

(2) Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,

(3) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

(4) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9 Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 10 Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Vertragsparteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die **Anhänge 1 bis 3** auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

§ 11 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

DocuSigned by:
Stephan Roth
A9293E1CC5E74C0...
Prokurist

Anhang 1

Software-as-a-Service-Produkte und Dienstleistungen des Auftragsverarbeiters

Software-as-a-Service-Produkte	**DSN port** mit den Modulen • **privacy** – Das Datenschutz-Managementsystem • **datenschutzBR** – Das Datenschutz-Managementsystem für Betriebsräte • **learning** – Das Learning Management System (LMS) Nachfolgend „Software“ oder „Anwendungen“.
Dienstleistungen	• Bereitstellung • Hosting • Wartung, Service und Support

Gegenstand, Art, Zweck und Dauer der Verarbeitung, Kategorien der personenbezogenen Daten und betroffenen Personen

Gegenstand der Verarbeitung	Bereitstellung von Software (Software-as-a-Service) einschließlich Hosting sowie Wartungs-, Service- und Supportdienstleistungen
Art und Zweck der Verarbeitung	Bereitstellung von Software (Software-as-a-Service) einschließlich Hosting sowie Wartungs-, Service- und Supportdienstleistungen
Kategorie der personenbezogenen Daten	• Benutzerdaten (z. B. Name, Vorname, geschäftliche E-Mail-Adresse) • Dienstleister- bzw. Vertragsdaten (z. B. Name, geschäftliche Kontaktdaten von Dienstleistern oder Vertragspartnern des Verantwortlichen) • Anlassbezogen aufgenommene Daten (z. B. Angaben zu Datenschutzvorfällen, Betroffenenanfragen, bestehenden Vertragsverhältnissen) • Logfiles, IDs und IP-Adressen der Benutzer Im Falle des LMS-Moduls learning zudem: • Daten von Schulungsteilnehmenden (z. B. Name, Vorname, Anrede, geschäftliche E-Mail-Adresse, Lernfortschritt)
Kategorien der betroffenen Personen	• Beschäftigte des Verantwortlichen

	• Dienstleister/Vertragspartner/Ansprechpartner des Verantwortlichen • Ggf. Betroffene oder sonstige Dritte im Falle der Dokumentation von Betroffenenanfragen oder Datenschutzvorfällen
Dauer der Verarbeitung	entspricht der Lizenzdauer

Kontaktdaten des/der Datenschutzbeauftragten

Datenschutzbeauftragte/r des Auftragsverarbeiters	Florian Wallrapp E-Mail: dsb@dsn-group.de

Anhang 2

Liste der beauftragten Unterauftragnehmer und der Verarbeitungsstandorte

UNTERAUFTRAGNEHMER	VERARBEITUNGSSTANDORT	BESCHREIBUNG DER VERARBEITUNG
PLUTEX GmbH, Hermann-Ritter-Str. 110, 28197 Bremen	Bremen	Bereitstellung von Servern in einem ISO/IEC 27001 zertifizierten Rechenzentrum in Bremen

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.

1. 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.

2. Maßnahmen zur Gewährung der Vertraulichkeit

2.1. 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.

2.2. 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.

2.3. 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.

2.4. 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.

2.5. 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.

2.6. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. Sonstige technische und organisatorische Maßnahmen

7.1. 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.

7.2. 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.

7.3. 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.