privacy train

Version vom 01.09.2021

Vertrag zur Auftragsverarbeitung privacy train (AVV privacy train)

zwischen der

datenschutz nord GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

als Lizenzgeber

(Auftragnehmerin)

und dem

privacy train Lizenznehmer

(Auftraggeberin)

Präambel

Die Auftragnehmerin stellt der Auftraggeberin das eLearning privacy train auf der Grundlage einer BASIC Lizenz oder einer LMS Lizenz zur Verfügung. Da die Auftragnehmerin in diesem Zusammenhang personenbezogene Daten im Auftrag und nach Weisung der Auftraggeberin verarbeitet, schließen die Parteien - in Ergänzung des Lizenzvertrags - den vorliegenden Vertrag zur Auftragsverarbeitung ab.

§ 1 Gegenstand und Dauer des Auftrags

(1) Die Auftragnehmerin führt die in der **Anlage A.1** beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Abschluss des Lizenzvertrags in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

§ 2 Weisungen der Auftraggeberin

(1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.

(5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin hat für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen getroffen und diese in **Anlage A.2.** dieses Vertrages dokumentiert. Die Sicherheitsmaßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

(3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Die Auftragnehmerin hat zum Zeitpunkt des Vertragsschlusses folgende Unterauftragnehmer beauftragt:

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
PLUTEX GmbH, Bremen	Bremen	Hosting, Managed Services

Der Lizenzgeber sichert zu, nur solche externen Hosting-Dienstleister einzusetzen, die zum Zeitpunkt der Unterbeauftragung nach ISO/IEC 27001 oder anderen gleichwertigen Standards zertifiziert sind. Weitere Unterauftragnehmer dürfen nur beauftragt werden, wenn die Auftragnehmerin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert wird. Ein Einspruch gegen die weitere Beauftragung darf nur aus wichtigem Grund erfolgen.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch die Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

§ 6 Kontrollrechte der Auftraggeberin

Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Bei Kontrollen vor Ort hat der Auftraggeber die dem Auftragnehmer hierdurch entstehenden Aufwendungen gemäß den üblichen Stundensätzen des Auftragnehmers zu vergüten. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße der Auftragnehmerin

Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a. eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
b. Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d. eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Die Auftraggeberin kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn die Auftragnehmerin einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und der Auftraggeberin aufgrund dessen die Fortsetzung der

Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

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

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was seit dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

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

9/17/2021

DocuSigned by:
Stephan Roth
A9293E1CC5E74C0...

A.1. Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	**LMS Lizenz:** Betrieb eines Learning Management Systems zur Durchführung von Online-Schulungen für die Beschäftigten der Auftraggeberin. **BASIC Lizenz:** Betrieb eines passwortgeschützten Internetzugangs zu den bestellten und auf dem Server der Auftragnehmerin bereitgestellten Kursinhalten.
Art und Zweck der Verarbeitung	**LMS Lizenz:** Nutzerverwaltung und Dokumentation des Schulungsstatus im LMS der Auftragnehmerin. **BASIC Lizenz:** Verwaltung eines Gruppenaccounts für den Zugang zu den bestellten Kursinhalten im LMS der Auftragnehmerin.
Art der personenbezogenen Daten	**LMS Lizenz:** Name, Vorname, Anrede, E-Mail-Adresse, Lernfortschritt (Kurs noch nicht begonnen, Kurs begonnen und Kurs abgeschlossen), Zeitpunkt der letzten Statusänderung, Unternehmenszugehörigkeit sowie ggf. Standort und Abteilung. IP-Adressen, soweit diese zur technischen Auslieferung der Inhalte erforderlich sind. Ein Tracking auf Basis der IP-Adressen erfolgt nicht. **BASIC Lizenz:** E-Mail-Adresse und ggf. Name und Vorname der Koordinatorin/des Koordinators auf Seiten der Auftraggeberin. IP-Adressen, soweit diese zur technischen Auslieferung der Inhalte erforderlich sind. Ein Tracking erfolgt nicht.
Kategorien betroffener Personen	**LMS Lizenz:** Beschäftigte der Auftraggeberin sowie Selbständige (Freelancer), die die Auftraggeberin bei sich einsetzt (Schulungsteilnehmer). **BASIC Lizenz:** Die Koordinatorin/der Koordinator auf Seiten der Auftraggeberin, Schulungsteilnehmer.
Name und Kontaktdaten der Datenschutzbeauftragten der Auftragnehmerin	Joanna Maxine Stünkel dsb@datenschutz-nord-gruppe.de

A.2. Technische und organisatorische Sicherheitsmaßnahmen

In diesem Anhang werden die technischen und organisatorischen Maßnahmen dokumentiert, die durch die Auftragnehmerin zur ordnungsgemäßen Erfüllung der erbrachten Dienstleistung umgesetzt werden.

1. Maßnahmen zur Pseudonymisierung personenbezogener Daten

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 nicht gespeichert bzw. umgehend anonymisiert.

2. Maßnahmen zur Verschlüsselung personenbezogener Daten

Die Schulungsplattform kann nur über eine Verbindung mit https-Verschlüsselung angesteuert werden. Administrative Zugriffe auf das Serversystem sind zudem nur aus dem Firmennetzwerk der Auftragnehmerin möglich.

3. Gewährleistung der Vertraulichkeit

Das Hosting der Software, die Administration der Server und Datenbanksysteme erfolgt durch einen nach ISO/IEC 27001 & DIN ISO 9001 zertifizierten Hosting-Dienstleister, der dem Auftragnehmer hoch verfügbare und sichere Managed Server bereitstellt.

a) Zutrittskontrolle

Maßnahmen zur Zutrittskontrolle (sollen Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren):

aa) Rechenzentrum:

Die Eingangstür zum Rechenzentrum (besonders widerstandsfähig) ist mit einer elektronischen Schließanlage ausgestattet (Schlüsselkarte und PIN-Code). Zutritte werden personenbezogen protokolliert. Das Rechenzentrum ist fensterlos und verfügt über eine Einbruchmeldeanlage.

bb) Büroraume:

Sämtliche Eingangstüren zu den Büroräumen sind mit elektronischen Schließanlagen ausgestattet (RFID-Chips). Auch während der Geschäftszeiten sind alle Eingangstüren verschlossen und können nur per Klinke von innen oder mit einem passenden Schlüssel geöffnet werden. Außerhalb der Geschäftszeiten werden die Büroräume mit einer Einbruchmeldeanlage überwacht (Alarmaufschaltung bei einem Sicherheitsdienst). Besucher dürfen sich nur in Begleitung eines Mitarbeiters in den Büroetagen aufhalten.

b) Zugangskontrolle

Maßnahmen zur Zugangskontrolle (sollen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können):

aa) Administrative Zugänge:

Administrative Zugänge zu der Schulungsplattform setzen die Eingabe eines Nutzernamens und eines Passworts voraus. Die Administratoren-Passwörter enthalten zwischen 11 und 20 Zeichen, bestehen aus großen und kleinen Buchstaben

sowie Sonderzeichen und Ziffern. Angemeldete Administratoren-Accounts werden nach spätestens 5 Minuten der Inaktivität automatisch abgemeldet. Serverseitig können administrative Tätigkeiten nur aus dem Unternehmensnetz der Auftragnehmerin durchgeführt werden.

bb) Client-Systeme:

Bei der Anmeldung am System werden Benutzername und Passwort abgefragt. Die verwendeten Passwörter müssen mindestens 8 Zeichen umfassen sowie aus großen und kleinen Buchstaben, Sonderzeichen und Ziffern bestehen. Passwörter müssen zudem alle 90 Tage geändert werden. Dabei sind die letzten 10 verwendeten Passwörter gesperrt. Nach 5 Minuten der Inaktivität wird das System gesperrt und kann nur mit Hilfe des Passworts wieder entsperrt werden. Alle Sicherheitsanforderungen der Zugangskontrolle werden systemseitig erzwungen.

c) Zugriffskontrolle

Maßnahmen zur Zugriffskontrolle (sollen 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):

Zugriffsrechte werden streng nach dem Need-to-Know-Prinzip auf der Grundlage von Berechtigungskonzepten vergeben.

Nutzerkonten können nur durch einen Administrator erstellt, gelöscht und verändert werden.

aa) LMS Lizenz

Jeder Nutzer kann nur seinen eigenen Lernstatus (Kurs bearbeitet, Kurs in Bearbeitung oder Kurs noch nicht bearbeitet) einsehen und hat keinen Zugriff auf die Daten der übrigen Nutzer (andere Nutzer sind für ihn unsichtbar). Der Lernstatus wird wie folgt protokolliert: Kurs bearbeitet (grün), Kurs in Bearbeitung (gelb) und Kurs noch nicht bearbeitet (grau). Jeder Statuswechsel wird zudem mit Datum und Uhrzeit protokolliert.

Es kann ein Koordinator ernannt werden, der mit erweiterten Rechten den Lernstatus aller Nutzer innerhalb des Mandanten einsehen darf.

bb) BASIC Lizenz

Die Auftraggeberin erhält einen einzelnen Nutzeraccount für den BASIC-Mandanten. Dieser Account ist so konfiguriert, dass im System lediglich die bestellen Kursmodule zugänglich sind. Es können weder die eigenen Profildaten noch die übrigen Nutzer in der Datenbank eingesehen werden.

d) Weitergabekontrolle

Maßnahmen zur Weitergabekontrolle (sollen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist):

Die Schulungsplattform kann nur über eine Verbindung mit https-Verschlüsselung angesteuert werden.

e) Trennungsgebot

Maßnahmen zur Umsetzung des Trennungsgebots (sollen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können):

Durch getrennte Datenbanken (LMS Lizenz) sowie eine logische Datentrennung (BASIC Lizenz) ist sichergestellt, dass die Daten einer Auftraggeberin getrennt von den Daten anderer Auftraggeberinnen verarbeitet werden.

4. Gewährleistung der Integrität (Eingabekontrolle)

Maßnahmen zur Eingabekontrolle (sollen gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind):

Das Anlegen und Verändern eines Nutzerkontos wird systemseitig protokolliert. Dasselbe gilt für den Lernstatus der teilnehmenden Nutzer (nur relevant für die LMS Lizenz, siehe hierzu auch Zugriffskontrolle).

5. Gewährleistung der Verfügbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen zur Verfügbarkeitskontrolle (sollen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind):

Der Datenbestand der Schulungsplattform wird täglich inkrementell und wöchentlich voll gesichert. Eine unterbrechungsfreie Stromversorgung verhindert, dass der Datenbestand bei einem plötzlichen Stromausfall Schaden nehmen kann. Das Rechenzentrum ist klimatisiert und verfügt über angemessene Brandschutzmaßnahmen. Sämtliche Systeme verfügen über einen aktuellen Virenschutz. Sicherheitsrelevante Softwareupdates werden unverzüglich installiert.

b) Auftragskontrolle

Maßnahmen zur Auftragskontrolle (sollen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können):

Mit allen Auftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO.

6. Gewährleistung der Belastbarkeit der Systeme

Es werden widerstandsfähige Systeme (Hard- und Software) eingesetzt, die im Hinblick auf die Speicher-, Zugriffs- und Leitungskapazitäten den zu erwartenden Beanspruchungen standhalten.

7. Regelmäßige Überprüfung der Maßnahmen

Die technischen und organisatorischen Maßnahmen werden laufend überprüft und im Bedarfsfall dem Stand der Technik angepasst.