Vertrag über Auftragsverarbeitung (AVV)

zwischen

– nachfolgend „Verantwortlicher“ genannt –

eLeDia GmbH

Wilhelmsaue 37

10713 Berlin

– nachfolgend „Auftragsverarbeiter“ genannt

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

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

(2) Sofern der Auftraggeber als kirchliche Einrichtung infolge des Selbstverwaltungsrechts der Kirchen gemäß Art. 91 Europäische Datenschutzgrundverordnung (DSGVO) nicht den Regeln der DSGVO, sondern dem Gesetz über den kirchlichen Datenschutz (KDG/Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) bzw. dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) unterliegt, unterwirft sich der Auftragnehmer dem Gesetz über den Kirchlichen Datenschutz (KDG)/Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) bzw. dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) und den insoweit zuständigen Aufsichtsbehörden, soweit dies gesetzlich vorgeschrieben ist. Sofern in dieser Vereinbarung auf die DSGVO Bezug genommen wird, sind die entsprechenden Normen des kirchlichen Datenschutzgesetzes mitgemeint.

§ 2 Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund 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, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.
(2) Die in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese 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. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 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. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(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) Sofern der Auftragsverarbeiter Daten des Verantwortlichen im Auftrag verarbeitet, die dem Schutzbereich des § 203 StGB bzw. einem Berufsgeheimnis unterliegen, darf der Auftragsverarbeiter nur dann auf derartige Daten zugreifen, soweit dies im Einzelfall erforderlich ist. Der Auftragsverarbeiter verpflichtet sich in diesem Zusammenhang, alle Personen, die im Rahmen der beauftragten Tätigkeit die in Satz 1 genannten Daten verarbeiten, auf die Geheimhaltung nach § 203 StGB zu verpflichten. Dem Auftragsverarbeiter ist bekannt, dass hinsichtlich der Daten, die dem Schutzbereich des § 203 StGB unterliegen, ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweigerung entscheidet der Berufsgeheimnisträger der Verantwortlichen. Dem Auftragsverarbeiter ist bekannt, dass die dem Berufsgeheimnis unterliegenden Daten, die sich im Gewahrsam des Auftragsverarbeiters zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 1, 3 StPO unterliegen. Einer Sicherstellung ist zu widersprechen. Der Verantwortliche ist unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 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 mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages 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. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

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

(4) 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.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der

Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

(6) Der Auftragsverarbeiter hat die Verpflichtung der weiteren mitwirkenden Personen und der Unterauftragsverarbeiter auf die Geheimhaltung gem. § 203 StGB und § 4 Abs. 5 dieses Vertrages sicherzustellen.

§ 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 gegebenenfalls 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. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a. Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
b. Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
c. Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d. 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. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.
(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

(1) Diesem Vertrag können mit Zustimmung aller Parteien 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.

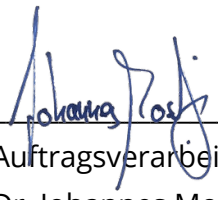
(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

_____

Ort, Datum

_____

Verantwortlicher



_____

Auftragsverarbeiter
Dr. Johannes Moskaliuk

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung

Bereitstellung einer Lernplattform

Art und Zweck der Verarbeitung

Der Auftragnehmer stellt für den Auftraggeber Software zur Bereitstellung von Lerninhalten und der Verarbeitung von Lernaktivitäten und Lernständen zur Verfügung. Die Software dient zur Ausbildung, Fort- und Weiterbildung sowie zur Kommunikation zwischen Anwendern. Der Auftragnehmer übernimmt für den Auftraggeber das Hosting, die Wartung und den Support der Lernplattform entsprechend den Leistungen in der Leistungsvereinbarung.

Art der personenbezogenen Daten

Vorname, Nachname, E-Mail des Nutzers, Anmeldename, wird i.d.R. durch Auftraggeber vergeben, persönliches Kennwort (kann geändert werden), Stadt, Land, weitere Daten, die der Nutzer in seinem Profil einstellt, belegte Kursveranstaltungen, Aktivitäten in Kursen, Forenbeiträge, bearbeitete Lernaktivitäten, Lernergebnisse, Protokolldaten über die Aktivität des Nutzers unter Angabe seiner IP-Adresse, durchgeführter Aktivitäten, Inhalt der Nutzereingabe und Zeitpunkt der Aktivität.

Ergänzungen des Verantwortlichen zu Art der bezogenen Daten:

Kategorien betroffener Personen: Nutzende der Lernplattform des Auftraggebers wie Mitarbeiter, Kunden des Auftraggebers, Schüler, Studierende, externe Trainer des Auftraggebers, Personen im Alter unter 16 Jahre.

Dauer der Verarbeitung

Die Dauer dieser Vertrag über Auftragsverarbeitung (AVV) entspricht der Laufzeit der am längsten laufenden Leistungs-vereinbarung zwischen Auftraggeber und Auftragnehmer.

Datenschutzbeauftragte/r des Verantwortlichen

Datenschutzbeauftragter des Auftragverarbeiters

Dr. Uwe Schläger, datenschutz nord GmbH, Zweigstelle Berlin-Charlottenburg, Kurfürstendamm 212, 10719 Berlin

Anhang 2

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

UNTERAUFTRAG–NEHMER	VERARBEITUNGS–STANDORT	BESCHREIBUNG DER VERARBEITUNG
Hetzner Online GmbH, Industriestr. 25D, 91710 Gunzenhausen	Verarbeitung erfolgt am Unternehmenssitz und in den Datenzentren in Falkenstein, Nürnberg und Helsinki.	Rechenzentrum, Webserver
Artfiles New Media GmbH, Zirkusweg 1, 20359 Hamburg	Verarbeitung erfolgt am Unternehmenssitz	Domainverwaltung, E-Mail-Dienst, Hosting BigBlueButton
UnterauftragnehmerAnschriftLeistungLinda und Sören Stein-mann GbR - Video-Stream-Hosting	Verarbeitung erfolgt am Unternehmenssitz	Video-Stream-Funktionalität
Talpaworld IT-Service-Team Herrenbrück-Köhler GbR, Johannesweg 52. 51061 Köln	Verarbeitung erfolgt am Unternehmenssitz	Installation, Monitoring und Wartung von BigBlueButton (be Hetzner Online GmbH)

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

Diese Anlage beschreibt die technischen und organisatorischen Maßnahmen, die der Auftragnehmer zum Schutz der verarbeiteten Daten getroffen hat. Für die von dem Auftragnehmer eingesetzten Unterauftrag-nehmer gelten gesonderte technische und organisatorische Maßnahmen, die auf Anfrage zur Verfügung gestellt werden.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Räumlichkeiten zu verwehren, in denen personenbezogene Daten verarbeitet werden:

- Die Räume verfügen über ein Schließsystem mit Sicherheitsschlössern.
- Ein Zutritt ohne Befugnis ist nicht möglich.
- Die Ausgabe von Schlüsseln wird dokumentiert.
- Der Zutritt von Besuchern ist nur in Begleitung durch Mitarbeiter zulässig.
- Die Gebäudereinigung erfolgt in Anwesenheit von Mitarbeitern während der Bürozeiten.

1.2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verarbeitet werden können:

- Es erfolgt eine Begrenzung der Zugangsberechtigten.
- Den Benutzern werden Benutzerrechte in Abhängigkeit von den von ihnen ausgeübten Funktionen zugewiesen.
- Eine Authentifizierung erfolgt mit Benutzernamen und Passwort.
- Es existieren Vorgaben zur Passwortgestaltung, -handhabung und -verwaltung.
- Die Arbeitsplätze, über die auf die Systeme der Kunden zugegriffen wird, sind als virtuelle Maschinen angelegt.
- Der Zugriff von anderen Orten außerhalb des Büros erfolgt über VPN und die virtuellen Maschinen des Mitarbeiters.
- Es wird auf allen PCs Antivirensoftware mit automatisierter Aktualisierung eingesetzt.

1.3. Zugriffskontrolle

Maßnahmen, 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 nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Zugriffsberechtigungen werden in Abhängigkeit von der Funktion eines Mitarbeiters vergeben.
- Die Anzahl der Administratoren ist begrenzt.
- Der Zugriff auf Anwendungen wird protokolliert.

- Für die Vernichtung papiergebundener personenbezogener Daten stehen Aktenvernichter zur Verfügung.

1.4. Trennungskontrolle

Die Verarbeitung von Daten verschiedener Auftraggeber erfolgt getrennt. Es wird zwischen Produktiv- und Testsystemen unterschieden.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1.5. Weitergabekontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet werden können:

- Der Zugriff auf personenbezogene Datensätze des Auftraggebers erfolgt nach Möglichkeit und nach Maßgabe der vertraglichen Vereinbarung über verschlüsselte Zugänge (https bzw. SSH).
- Die Weitergabe von Daten ist nur nach Maßgabe der vertraglichen Vereinbarungen und auf Weisung des Auftraggebers zulässig.
- Es werden Logprotokolle erzeugt.
- Die Abfrage und Übertragung personenbezogener Daten durch Anwender erfolgt verschlüsselt mittels Webbrowser (https). Passwörter der Nutzer werden in der Datenbank nach Möglichkeit verschlüsselt abgelegt.

1.6. Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme verarbeitet worden sind:

- Es gibt ein Protokoll der Eingaben.
- Es werden serverseitige Logprotokolle über Nutzerzugriffe geführt.
- Es besteht ein Berechtigungskonzept.
- Die Protokollierung erfolgt im Rahmen der Funktionen in den vom Auftraggeber beauftragten Anwendungsprogramme.
- Sofern ein automatisierter Austausch personenbezogener Daten zwischen Anwendungen des Auftraggebers und des Auftragnehmers erfolgen (z.B. Authentifizierungssysteme, Anbindung an HR-Systeme), werden diese Übertragungen über sichere Transportwege vorgenommen. Für den Austausch von Daten in manueller Weise stellt der Auftragnehmer einen geschützten Upload auf Anfrage zur Verfügung.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.7. Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Datensicherung: Es erfolgt eine tägliche Sicherung der Daten. Die Daten werden nach erfolgter Sicherung auf getrennten Servern abgelegt.

- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Die Wiederherstellung der Daten aus den Backups kann jederzeit beauftragt werden. Die Wiederherstellbarkeit wird exemplarisch bzw. nach gesonderter Beauftragung durch den Auftraggeber geprüft.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Die in dieser Anlage beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen werden mindestens einmal jährlich geprüft und bei Bedarf angepasst. Bei Feststellung eines sicherheitsrelevanten Vorfalls werden die getroffenen Maßnahmen umgehend geprüft und im erforderlichen Umfang angepasst.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO): Die Konfiguration des Anwendungsprogramms erfolgt in Abstimmung zwischen dem Auftraggeber und dem Auftragnehmer. Der Auftraggeber erhält Administrationszugriff auf das System und kann die entsprechenden Einstellungen über die Administrationsoberfläche des Anwendungsprogramms jederzeit selbst anpassen.

Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Auswahl von Auftragsverarbeitern erfolgt sorgfältig unter Beachtung der Bestimmung des Art. 28 DSGVO.
- Weisungen an die beauftragten Auftragsverarbeiter erfolgen in Textform.
- Der Auftragnehmer hat einen fachkundigen Datenschutzbeauftragten benannt.
- Der Auftragnehmer arbeitet nur mit Auftragsverarbeitern zusammen, die einen Datenschutzbeauftragten benannt haben.
- Die Mitarbeiter des Auftragnehmers werden schriftlich auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet.
- Die Mitarbeiter des Auftragnehmers werden regelmäßig über die Verpflichtungen unterrichtet, welche sich aus der Auftragsverarbeitung ergeben.
- Sämtliche personenbezogenen Daten werden nach Beendigung des Auftrags bzw. nach Ablauf gesetzlicher Aufbewahrungsfristen gelöscht.