Anlage 1 I Vereinbarung über die Auftragsdatenverarbeitung

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2

Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3

Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4

Vorrang

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

Klausel 5

Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

PFLICHTEN DER PARTEIEN

Klausel 6

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Klausel 7

Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung 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 dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) 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 sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer

Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

c) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

a) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

b) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln 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 des Auftragsverarbeiters berücksichtigen.

c) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

d) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die unter https://elearnio.com/de/unterauftragsverarbeiter/ aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 4 Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Auftragsverarbeiter gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. Die Parteien erklären sich damit einverstanden, dass der Auftragsverarbeiter durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 7 nachkommt. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter gemäß diesen Klauseln unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche — sollte der Auftragsverarbeiter faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Hinweis zur Gültigkeit:

Die zum Zeitpunkt des Vertragsschlusses gültige Version der Liste der Unterauftragsverarbeiter ist die Version v1.3 mit Stand 23.06.2025, abrufbar unter https://elearnio.com/de/unterauftragsverarbeiter/.

7.8. Internationale Datenübermittlungen

f) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

g) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8

Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz- Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679] zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

ANLAGE

ANHANG I

LISTE DER PARTEIEN

Verantwortlicher:

Name:

Adresse:

Name, Funktion und Kontaktdaten der Kontaktperson:

Unterschrift und Datum:

Auftragsverarbeiter:

elearnio GmbH
David-Gilly-Straße 1
14469 Potsdam

Name, Funktion und Kontaktdaten der Kontaktperson:

Sascha Meißner, Managing Director, sascha@elearnio.com

Unterschrift und Datum:

Potsdam, den

ANHANG II

BESCHREIBUNG DER DATENÜBERMITTLUNG

Kategorien betroffener Personen, deren personenbezogene Daten übermittelt werden

- *Beschäftigte (Angestellte, Arbeiter, Auszubildende, Leiharbeitnehmer, Praktikanten, Bewerber) des Auftraggebers und aller mit dem Auftraggeber verbundenen Unternehmen*
- *Kunden*
- *Geschäftspartner*
- *Andere Personen, die auf Grund eines Vertrages in Kontakt mit der Lernplattform kommen*
- *Nutzer des Verantwortlichen*

Kategorien der übermittelten personenbezogenen Daten

Art der Daten	***Detailbeschreibung***	***Zweck***
Technische Daten	*IP-Adresse des letzten Login*	*Verifikation des Login*
Stammdaten der Nutzer	*Name, Vorname, Geschlecht, Kostenstelle, E-Mailadresse, Nutzername, Geburtstag, Personalnummer, E-Mailadresse der Führungskraft, Position, Team, Abteilung, Standort, Business Unit, Geschäftsbereich, LinkedIn Profil (Link), Nutzerstatus (Preboarding, Onboarding, Aktiv, Abwesend, Inaktiv), Karrierestufe, Firma, Anrede, Anstelldatum*	*Stammdatenspeicherung zur Identifizierung, Ansprache und Verwaltung der Nutzer*
Fortschritte + Ergebnisse von Trainings (Kurse, Live-Trainings, Lernpfade)	*Benutzeridentifikationsnummer, Name, Vorname, E-Mailadresse, Benutzername, Datum und Uhrzeit zugewiesener + abgeschlossener Trainings, prozentualer Fortschritt, Abschlussquote, Bestanden (ja / nein) und prozentuales Ergebnis, im Rahmen einer Wissensabfrage gegebene Antworten, im Rahmen einer Feedback-Befragung gegebene Antworten, Lernzeit, Gamification Punkte, erzielte Zertifikate (soweit solche erteilt werden sollen), besuchte Module im Training, Datum und Uhrzeit der Nutzeranlage + der zuletzt erfolgten Anmeldung*	*Auswertung der Lernstände*

Häufigkeit der Übermittlung

- *Kontinuierliche Übermittlung*

Art der Verarbeitung gemäß Art. 4 Nr. 2 DSGVO:

Im Rahmen des Auftrags verarbeitet der Auftragnehmer personenbezogene Daten im Sinne von Art. 4 Nr. 2 DSGVO. Die durchgeführten Verarbeitungsschritte umfassen insbesondere:

- *Erheben & Erfassen: Aufnahme von Nutzerdaten bei der Registrierung.*
- *Organisation & Ordnen: Verwaltung von Benutzerkonten, Zuweisung zu Schulungen.*
- *Speicherung: Speicherung von Stammdaten und Lernfortschritten.*
- *Anpassung oder Veränderung: Aktualisierung von Nutzerinformationen.*
- *Auslesen & Abfragen: Abruf von Nutzerinformationen durch autorisierte Personen.*
- *Verwendung: Bereitstellung von Inhalten in der Lernplattform.*
- *Einschränkung: Deaktivierung oder Sperrung von Benutzerkonten.*
- *Löschen oder Vernichtung: Datenlöschung nach Beendigung der Vertragsbeziehung oder auf Anweisung des Verantwortlichen.*

Zweck(e) der Datenübermittlung und Weiterverarbeitung

- *Bereitstellung der elearnio Plattform*

Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

- *Die Daten werden zur Erfüllung der vertraglichen Hauptleistungspflichten des Datenimporteurs gespeichert und bis zum Zweckfortfall, alternativ entsprechend der gesetzlichen bestimmten Vorhaltepflichten gespeichert und danach gelöscht.*

ANHANG III

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Die Services des Auftragsverarbeiters werden durch eine so genannte Software-as-a-Service (SaaS) Lösung erbracht. Die Software wird in einer Infrastruktur des in Anhang IV bestimmten Dritt-Anbieters Amazon Web Services ("AWS") betrieben. In diesem Verhältnis, sowie elearnio intern sind die folgenden technischen und organisatorischen Maßnahmen vereinbart:

1. ***Datenschutzkonzept, Betroffenenrechte, Technikgestaltung und Datenschutz auf Mitarbeiterebene***
    1. *Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:*
        - *Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird, sowie anlassbezogen und mindestens halbjährlich evaluiert wird.*
        - *Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.*
        - *Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen*
        - *Der Schutz von personenbezogenen Daten wird 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).*
        - *Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.*
        - *Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.*
        - *Die an Mitarbeiter ausgegebenen Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.*
        - *Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass es den Schutz personenbezogener Daten beachtet.*

2. Zugangskontrolle

1. *Maßnahmen, mit denen Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:*
    - *Es wird ein „papierloses Büro“ geführt und Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.*
    - *Es werden, bis auf die Arbeitsplatzrechner und mobile Geräte, keine Datenverarbeitungsanlagen in den eigenen Geschäftsräumlichkeiten unterhalten. Die Daten des Auftraggebers werden bei externen Hosting-Anbieter unter Beachtung der Vorgaben für Auftragsverarbeitung gespeichert.*
    - *Es bestehen Zutrittsregelungen für betriebsfremde Personen.*
    - *Es findet eine Personenkontrolle beim Pförtner oder am Empfang statt.*
    - *Besucher müssen sich am Empfang melden, werden verzeichnet und von einem Mitarbeiter abgeholt.*
    - *Der Zutritt jeglicher Personen (auch Mitarbeiter) muss durch autorisiertes Personal im Voraus genehmigt werden und wird durch eine Personenkontrolle überprüft.*
    - *Die Besucher werden protokolliert.*
    - *Es gibt eine Tragepflicht von Berechtigungsausweisen.*
    - *Das Betriebsgebäude des Auftragnehmers ist in unterschiedliche Zutrittsbereiche eingeteilt.*
    - *Der Zutritt zu den Datenverarbeitungsanlagen (EDV-Räumlichkeiten am Serverstandort) ist unbefugten Personen vollständig verwehrt und nur zutrittsberechtigten Mitarbeitern gewährt. (AWS Hosting Center Frankfurt)*
    - *Die Infrastruktur wird bei Amazon Web Services (AWS, Frankfurt, DE) gehostet. AWS erfüllt höchste Sicherheitsstandards, darunter ISO 27001, SOC 2, redundante Rechenzentren mit Zutrittskontrollen, Videoüberwachung und biometrischer Zugangssicherung.*
    - *Es ist eine Alarmanlage installiert.*
    - *Gebäudeschächte sind gegen Zugang durch Unbefugte abgesichert.*
    - *Die Fenster sind gesichert (falls Erdgeschoss oder sonstige Einbruchgefahr besteht).*
    - *Der Zugang ist sowohl durch ein automatisches Zugangskontrollsystem gesichert, als auch durch ein manuelles Schließsystem mit Sicherheitsschlössern gesichert.*
    - *Es besteht eine Regelung für Schlüssel oder Zugangskarten (Protokollierung der Ausgabe).*
    - *Die Zugänge werden videoüberwacht.*

3. Zutrittskontrolle

1. *Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:*
    - *Es gibt ein Rechtekonzept, bzw. ein Rollenkonzept, mit dem die Zutrittsberechtigungen der Mitarbeiter, Beauftragter und sonstiger Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind. (AWS IAM)*
    - *Das Least-Privilege-Prinzip wird angewendet. Admin-Zugänge zu Servern und Datenbanken sind auf eine minimale Anzahl autorisierter Personen beschränkt und durch Multi-Faktor-Authentifizierung (MFA) geschützt.*
    - *Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.*
    - *Es gibt ein Passwortkonzept, dass festlegt, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.*
    - *Es wird eine Passwort-Management-Software verwendet.*
    - *Anmeldungen in den Verarbeitungssystemen werden protokolliert.*
    - *Es wird eine Anti-Viren-Software eingesetzt. (AWS GuardDuty)*
    - *Es werden Hardware-Firewalls eingesetzt. (AWS WebApplicationFirewall)*

- *Es werden Software-Firewalls eingesetzt. (AWS WebApplicationFirewall)*
- *Die Website und/oder Zugänge zu Online-Software-Angeboten sind durch eine aktuelle TLS/SSL-Verschlüsselung geschützt.*
- *Die internen Systeme werden per Firewall sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt.*
- *Es gibt eine Begrenzung der Fehlversuche beim Login auf betriebsinterne Systeme (z.B. Sperrung von Logins oder IP-Adressen).*
- *Soweit technisch unterstützt, wird die Zwei-Faktor-Authentifizierung genutzt.*
- *Beim Zugriff auf betriebsinterne Systeme von außen (z.B. bei Fernwartung) werden verschlüsselte Übertragungstechnologien verwendet (z.B. VPN).*
- *Externe Schnittstellen sind gegen unberechtigte Hardwarezugriffe gesperrt (z.B. Sperrung von USB-Schnittstellen).*
- *Es werden Serversysteme und Dienste eingesetzt, die über Intrusion-Detection-Systeme verfügen. (AWS WAF)*
- *Die Cloud-Architektur nutzt AWS Virtual Private Cloud (VPC), Security Groups und Firewalls, um interne und öffentliche Bereiche strikt zu trennen.*
- *Mobile Datenträger werden verschlüsselt.*

4. Zugriffskontrolle und Eingabekontrolle

1. *Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, eingegeben, gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, die es erlauben die Verarbeitungsvorgänge nachträglich nachzuvollziehen:*
    - *Es gibt ein Rechtekonzept, bzw. ein Rollenkonzept, mit dem die Zugriffsberechtigungen der Mitarbeiter, Beauftragter und sonstiger Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.*
    - *Protokollierung jedes einzelnen Schrittes der Datenverarbeitung, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.*
    - *Zugriffe auf die personenbezogenen Daten erfolgt ausschließlich von Standorten innerhalb des EWR (Frankfurt am Main).*
    - *Die Zugriffe der Mitarbeiter auf Daten werden protokolliert. Sofern einzelne Zugriffe nicht protokolliert werden, wird sichergestellt, dass die nachvollziehbar ist, wer auf welche Daten wann Zugriff hatte (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).*
    - *Protokollierung jedes einzelnen Schrittes, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.*
    - *Datenträger werden sicher aufbewahrt.*
    - *Ein Session-Timeout-Mechanismus ist implementiert, der nach 5 Tagen Inaktivität die Sitzung automatisch beendet und einen erneuten Login erfordert.*
    - *Es liegt ein Lösch- und Entsorgungskonzept entsprechend der DIN 66399 mit festgelegten Zuständigkeiten und Protokollierungspflichten vor. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.*
    - *Die Verarbeitung von Daten, die nicht gelöscht werden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird durch Sperrvermerke und Aussonderung eingeschränkt.*
    - *Formulare, von denen Daten in automatisierte Verarbeitungen übernommen worden sind, werden aufbewahrt, wenn dem eine Weisung von Auftraggebern zugrunde liegt oder die Papierform eine rechtliche Relevanz hat.*

5. Weitergabekontrolle

1. *Maßnahmen, die 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:*
    - *Keine intern / lokal gehosteten Systeme. Zugriff auf Cloud-basierte System- /Toolwelt erfolgt ausschließlich über SSL gesicherte Verbindungen (https)*
    - *Es werden die für die Abgabe von Datenträgern berechtigten Personen und die Empfangsberechtigten bestimmt.*
    - *Es existieren ein Bestandsverzeichnis und eine Bestandskontrolle der Datenträger.*
    - *Es wird festgelegt für welchen Zeitraum der Zugriff auf die Daten möglich ist.*
    - *Es wird eine Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen erstellt und kontrolliert.*
    - *Sofern erforderlich, möglich und zumutbar, werden Daten in anonymisierter Form bzw. in pseudonymisierter Form weitergegeben.*
    - *Es wird eine E-Mail-Verschlüsselung eingesetzt, sofern diese möglich, zumutbar und vom Kommunikationspartner gewünscht oder sonst als erforderlich und/oder angemessen zu betrachtet ist.*
    - *PGP Verschlüsselung bei Signed Commits in der Softwareentwicklung.*
    - *Die Verschlüsselung des Speichermediums von Laptops erfolgt durch die in macOS integrierte Verschlüsselungstechnologie FileVault.*
    - *Gesichertes WLAN ohne Gastfunktion mit WPA3-Verschlüsselung.*

6. Auftragskontrolle

1. *Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von Auftraggebern verarbeitet werden können:*
    - *Verpflichtung von Mitarbeitern und Beauftragten auf die Beachtung von Weisungen.*
    - *Fernwartungszugriffe sind nur nach freigegebenem Antrag und unter Protokollierung (Logging) zulässig. Alle externen Zugriffsvorgänge werden dokumentiert und regelmäßig überprüft.*
    - *Schriftliche Festlegung und Dokumentation der Weisungen.*
    - *Die vertraglichen und gesetzlichen Vorgaben für die Beauftragung von Unterauftragsverarbeitern werden durch Abschluss von AV-Verträgen und Sicherstellung notwendiger Garantien sowie deren Kontrolle beachtet.*
    - *Unterauftragsverarbeiter werden nach strengen Datenschutz- und Sicherheitskriterien ausgewählt. Alle Dienstleister müssen angemessene Zertifizierungen (z. B. ISO 27001, SOC 2) oder gleichwertige Sicherheitsnachweise erbringen.*
    - *Es wird sichergestellt, dass Daten nach Beendigung des Auftrags zurückgegeben oder vernichtet werden.*

7. Verfügbarkeitskontrolle

1. *Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:*
    - *Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind, Belastbarkeitstests und Hardwaretests unterliegen, über einen DDoS-Schutz verfügen sowie eine unterbrechungsfreie Stromversorgung bieten.*
    - *Es werden Serversysteme und Dienste eingesetzt, die ein Backupsystem an anderen Orten, bzw. zumindest in anderen Brandabschnitten bieten, auf dem die aktuellen Daten vorgehalten werden und so ein lauffähiges System auch im Katastrophenfall zur Verfügung stellen.*

- *Es werden Serversysteme und Dienste eingesetzt, die sowohl über Feuchtigkeitsmelder verfügen, als auch über Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte im EDV Raum verfügen.*
- *Es werden Serversysteme und Dienste eingesetzt, die ein zuverlässiges und kontrolliertes Backupkonzept & Recoverykonzept bieten. Backups erfolgen täglich und monatlich. Die Backups werden verschlüsselt.*
- *Backups werden ebenfalls für die Datenverarbeitung auf Arbeitsplatzrechnern sowie Mobilgeräten erstellt und kontrolliert. Backups erfolgen laufend. Die Backups werden verschlüsselt.*
- *Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent überwacht.*

8. Gewährleistung der Zweckbindung/Trennungsgebot

1. *Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:*
    - *In AWS-Datenzentren, einschließlich des Standorts in Frankfurt (eu-central-1), wird physische Trennung als Teil der Redundanz- und Verfügbarkeitsstrategien verwendet. AWS verwendet mehrere Schichten physischer und infrastruktureller Maßnahmen, um sicherzustellen, dass Daten sicher und verfügbar sind.*
    - *Ein Übergriff durch nichtberechtigte Personen oder Prozesse wird durch ein Berechtigungskonzept verhindert.*
    - *Im Fall pseudonymisierter Speicherung, werden die Zuordnungsschlüssel getrennt von den Daten gespeichert und gegen eine unberechtigte oder nicht vom Verarbeitungsprozess vorgesehene Verknüpfung gesichert.*
    - *Produktiv- und Testsysteme werden getrennt.*