# Allgemeine Geschäftsbedingungen der EBERTZ DATENSCHUTZ GmbH für SaaS „Nutzung Software as a Service“.

**§ 1 Anwendungsbereich, ausschließliche Geltung, Änderungen der Geschäftsbedingungen**

(1) Die EBERTZ DATENSCHUTZ GmbH, HRB 8970, (im nachfolgenden EBERTZ DATENSCHUTZ genannt) ist ein Beratungsunternehmen mit Hauptsitz in Mittenaar, welches auf Beratung im Bereich der Informationssicherheit und des Datenschutzes spezialisiert ist. Zum Leistungsumfang gehören (Stand Januar 2024):
- die Bereitstellung eines Datenschutzmanagement Systems (Robin Data)
- die Bereitstellung eines Whistleblowing Case Management Systems (Whistleblowing Software)
- die Bereitstellung einer elearning Plattform zur Mitarbeiter-Sensibilisierung (Coursepath)

Die Bereitstellung o.g. Software-Produkte erfolgt als weisungsgebundene Dienstleistung im Sinne der EU-Datenschutzgrundverordnung, für den Auftraggeber. Die erforderliche Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO (siehe Anlagen 1-4) wird zwischen Auftraggeber und EBERTZ DATENSCHUTZ im Rahmen der Beauftragung geschlossen.
Diese AGB gelten zwischen der EBERTZ DATENSCHUTZ und dem jeweiligen Kunden. Die EBERTZ DATENSCHUTZ ist nur Vermittler der SaaS-Nutzungsberechtigung und nicht der Software-Entwickler (nachfolgend Provider genannt).

(2) Das Angebot der EBERTZ DATENSCHUTZ richtet sich ausschließlich an Unternehmer, die in ihrer gewerblichen, freiberuflichen oder selbständigen beruflichen Tätigkeit und nicht zu privaten Zwecken handeln. Die EBERTZ DATENSCHUTZ erbringt keine Leistungen an Verbraucher im Sinne des § 13 BGB.

(3) Die vorliegenden Allgemeinen Geschäftsbedingungen für SaaS (AGB) sind Vertragsbestandteil und gelten für alle, somit auch zukünftigen Geschäftsbeziehungen zwischen der EBERTZ DATENSCHUTZ und ihren Kunden im Bereich SaaS (Softwaremiete) Die AGB werden von ihnen in vollem Umfang in der zum Zeitpunkt des Vertragsschlusses geltenden Fassung akzeptiert. Von diesen Bedingungen abweichenden Regelungen, insbesondere auch etwaigen AGB des Kunden, wird hiermit widersprochen.

(4) Soweit die EBERTZ DATENSCHUTZ ihre AGB aktualisiert, wird sie den Kunden unverzüglich über die neue Fassung informieren. Die neuen AGB werden Vertragsbestandteil, wenn der Kunde ihnen zugestimmt hat oder den AGB nicht innerhalb von zwei Wochen nach Mitteilung der Aktualisierung widerspricht.

**§ 2 Vertragsgegenstand**

(1) Über den Provider vermittelt die EBERTZ DATENSCHUTZ an ihre Kunden SaaS-Dienstleistungen (software as a service) über das Medium Internet im Bereich datenschutzrechtlicher Software.

(2) Vertragsgegenstand ist die Überlassung der jeweiligen Software Nutzung.

**§ 3 Angebot**

(1) Alle Angebote der EBERTZ DATENSCHUTZ sind freibleibend, sofern im Angebot nicht ausdrücklich etwas anderes bestimmt wird.

(2) Die Vertragsannahme kommt durch die Auftragsbestätigung der EBERTZ DATENSCHUTZ zustande.

**§ 4 Leistungen**

(1) EBERTZ DATENSCHUTZ vermietet dem Kunden als Vermittler die im Angebot bezeichnete Software. Der Quellcode ist nicht Vertragsgegenstand und wird nicht mit ausgeliefert.

(2) Im digitalen Benutzerhandbuch bzw. den sonstigen Dokumentationen der Softwaren ist im Einzelnen beschrieben, welche Funktionen und Leistungen die Software bei vertragsgemäßer Nutzung hat. Für die vereinbarte Beschaffenheit der Software sowie die bestimmungsgemäße Verwendung ist insoweit allein die jeweilige Beschreibung maßgeblich. Öffentliche Äußerungen, Anpreisungen oder Werbung stellen keine Beschaffenheitsangabe der Softwareprogramme dar.

**§ 5 Nutzungsvoraussetzung für SaaS-Leistungen**

(1) Für die Bestellung und Nutzung der SaaS-Leistungen müssen Kunden über einen Computer verfügen (z. B. Desktop-Computer, Laptop, Notebook oder Tablet), der über eine ausreichend schnelle Internetverbindung verfügt (z. B. einen DSL-Anschluss).

(2) Die Nutzung der SaaS-Leistungen über Smartphones ist prinzipiell möglich. Es bestehen aber technisch bedingte Einschränkungen in der Nutzbarkeit, da die Angebote der Software aufgrund der komplexen, aber notwendigen Datenerfassungen nicht auf die Nutzung von Smartphones optimiert sind.

(3) Bei der Nutzung der Software kann der Kunde je nach gebuchtem Paket ein auf branchenmerkmalen und weiteren Attributen ein in Teilen und auf Basis von Vorlagen vorkonfiguriertes Datenschutz-Management-System erhalten oder entsprechende Vorlagen manuell importieren. Dieses vorkonfigurierte System wir auf Basis definierter Algorithmen nach bestem Wissen und Gewissen erzeugt und die Genauigkeit stetig verbessert. Es wird ausdrücklich darauf hingewiesen, dass eine rechtliche Beratung oder Prüfung nicht Bestandteil der gemieteten Software ist. Der Kunde muss selbst oder durch einen Fachmann alle durch die Datenschutzsoftware bereitgestellten Vorlagen prüfen, häufig an wenigen Stellen anpassen (z. B. Ergänzung von Informationen zur Organisation) und freigeben.

**§ 6 Softwareüberlassung**

(1) EBERTZ DATENSCHUTZ stellt über den Provider dem Kunden für die Dauer des jeweils geschlossenen Vertrags das Online-Portal in der jeweils aktuellen Version über das Internet entgeltlich zur Verfügung. Zu diesem Zweck richtet der Provider das Online-Portal auf einem Server ein, der über das Internet für den Kunden erreichbar ist.

(2) Der jeweils aktuelle Funktionsumfang des Online-Portals ergibt sich aus der aktuellen Leistungsbeschreibung der jeweiligen Datenschutz-Management-Software.

(3) Der Provider entwickelt das Online-Portal laufend weiter und wird dieses durch Updates und Upgrades verbessern.



EBERTZ DATENSCHUTZ GmbH | Ober den Wiesen 17 | 35756 Mittenaar | Amtsgericht Wetzlar HRB 8970
Geschäftsführer: Inge Ebertz und Lars Ebertz, Diplom-Ingenieur | E-Mail: info@ebertz-datenschutz.de | www.ebertz-datenschutz.de

**§ 7 Nutzungsrechte**

(1) Das Nutzungsrecht gilt so lange, wie der Vertrag zwischen Kunde und EBERTZ DATENSCHUTZ Bestand hat. Nach Erlöschen des Vertrags erlischt auch das Nutzungsrecht.

(2) Die gewährten Nutzungsrechte gelten aufschiebend, bis die vollständige Bezahlung der vereinbarten Leistungsvergütung zwischen Kunde und EBERTZ DATENSCHUTZ durchgeführt wurde.

(3) Der Provider erbringt die vertraglich vereinbarten Leistungen mit größtmöglicher Sorgfalt. Sollten Mängel auftreten sind die durch den Kunden an die EBERTZ DATENSCHUTZ unverzüglich anzuzeigen. Die EBERTZ DATENSCHUTZ leitet diese dann an den Provider weiter.

(4) Die in der Software bereitgestellten Vorlagen und Muster basieren auf anwaltlich, oder andere Fachexperten geprüften Vorlagen und werden durch ein intelligentes algorithmisches Verfahren in dem jeweiligen Mandanten, nach der Anmeldung oder auch auf Basis speziell zu startenden Funktionen, angelegt. Der Provider übernimmt keine Garantie für deren Vollständigkeit, die Korrektheit oder Passung auf die individuelle Situation des Kunden.

(5) Leistungen im Bereich der datenschutzrechtlichen Bestandaufnahme zur Erstellung des Datenschutzmanagementsystem führt der Provider immer mit größtmöglicher Sorgfalt und Genauigkeit durch. Allerdings kann es sein, dass der Provider zum Zeitpunkt der Analyse nicht alle relevanten Daten und Informationen vorliegen, um alle Implikationen umfassend bewerten zu können. Der Provider übernimmt keine Garantie für die Vollständigkeit der durchgeführten Analyse.

(6) Bei angezeigten und nachgewiesenen Mängeln führt der Provider eine Mängelbeseitigung nach eigenem Ermessen und in angemessener Zeit durch. Uns stehen dabei mindestens zwei Versuche zu. Im Falle eines endgültigen Scheiterns der Mängelbeseitigung kann der Kunde mindern oder vom Vertrag zurücktreten.

**§ 8 Nutzungspflichten**

(1) Der Kunde ist auf die Einhaltung aller geltenden Gesetze, insbesondere der Vorschriften des Strafgesetzbuches verpflichtet. Ferner hat er sicherzustellen, dass durch seine Nutzung des Service keine Rechte Dritter verletzt werden. In Übereinstimmung mit den gesetzlichen Bestimmungen versichert der Auftraggeber ferner, keine sitten- oder rechtswidrigen Inhalte über den Service bereitzustellen. Dies beinhaltet insbesondere alle Inhalte (einschließlich Mitgliedsnamen usw.)
- die falsch, unzutreffend oder irreführend sind;
- die beleidigend, rassistisch, sexistisch, pornografisch oder obszön sind;
- die dem Ruf von EBERTZ DATENSCHUTZ und dem Provider schaden können;
- die geeignet sind, Urheberrechte, Patente, Marken oder andere Rechte an geistigem Eigentum, die Rechte am eigenen Bild und andere persönlichen Rechte oder Rechte Dritter zu verletzen.

(2) Alle dem Kunden zur Verfügung gestellten Zugangsdaten sind streng vertraulich zu behandeln. Besteht der Verdacht oder die Gewissheit, dass Zugangsdaten in den Besitz von unberechtigten Dritten gelangt sind, ist EBERTZ DATENSCHUTZ hiervon unverzüglich in Kenntnis zu setzen.

(3) Besteht der Verdacht einer Kompromittierung der Zugangsdaten, so ist der Provider berechtigt, nach eigenem Ermessen und ohne vorherige Ankündigung die Zugangsdaten zu Ändern und den zugehörigen Account zu deaktivieren. Der Provider wird den Kunden über die EBERTZ DATENSCHUTZ umgehend informieren und auf Anfrage dem Kunden die neuen Zugangsdaten unverzüglich mitteilen. Der Kunde hat keinen Anspruch darauf, dass die ursprünglichen Zugangsdaten wiederhergestellt werden.

(4) Der Kunden haftet für alle Handlungen Dritter, die auf der unrechtmäßigen Verwendung von Zugangsdaten beruhen.

**§ 9 Haftung**

(1) Ebertz Datenschutz, der Provider sowie deren gesetzlichen Vertreter und Erfüllungsgehilfen haften nur für Vorsatz. Nur wenn wesentliche Vertragspflichten (folglich solche Pflichten, deren Einhaltung für die Erreichung des Vertragszwecks von besonderer Bedeutung ist) betroffen sind, wird auch für grobe oder leichte Fahrlässigkeit gehaftet. Dabei beschränkt sich die Haftung auf den vorhersehbaren, vertragstypischen Schaden.

(2) Der vorstehende Haftungsausschluss betrifft nicht die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit. Auch die Vorschriften des Produkthaftungsgesetzes bleiben von diesem Haftungsausschluss unberührt.

(3) Verstößt der Auftraggeber oder der Dritte gegen die in Abschnitt 6 dargelegten Verpflichtungen, so ist der Auftraggeber dem Provider gegenüber zum Ersatz des hierdurch entstehenden Schadens einschließlich notwendiger Rechtsverfolgungskosten verantwortlich. Erfolgende Urheberrechtsverletzungen durch den Dritten werden so behandelt, als wären diese durch den Auftraggeber selbst erfolgt.

**§ 10 Vergütung**

(1) Sämtliche vereinbarten für SaaS werden entweder zum Beginn eines Kalendermonats in Rechnung gestellt (Datenschutz-Software) oder als Jahrespauschale im voraus berechnet (Whistleblower Software).

(2) Das Zahlungsziel beträgt i. d. R. 14 Tage, sofern nichts anderweitiges schriftlich mit dem Kunden vereinbart wurde.

(3) Die monatlichen Zahlungen erfolgen in der Regel über ein vom Kunden zu erteilendem SEPA-Basis-Lastschriftmandat. Die Abbuchung erfolgt durch die EBERTZ DATENSCHUTZ termingerecht zum Ende des vereinbarten Zahlungsziels. Zahlung durch Überweisung ist in Ausnahmefällen möglich und muss vor Auftragsvergabe schriftlich vereinbart werden.

**§ 11 Verschwiegenheitspflicht**

(1) Die EBERTZ DATENSCHUTZ ist verpflichtet, über alle Informationen zum Kunden, die der EBERTZ DATENSCHUTZ im Zusammenhang mit der Nutzung der SaaS, Stillschweigen zu bewahren.

(2) Die Verschwiegenheitspflicht besteht nicht, wenn und soweit die EBERTZ DATENSCHUTZ vom Kunden von dieser Verpflichtung entbunden wurde.

(3) Die Verschwiegenheitspflicht besteht auch dann nicht,
- soweit die Offenlegung von Informationen zur Wahrung berechtigter Interessen des Auftragnehmers auch unter Berücksichtigung etwaiger entgegenstehender Interessen des Auftraggebers unerlässlich ist;
- soweit der Auftragnehmer nach den Versicherungsbedingungen seiner Berufshaftpflicht zur Information und Mitwirkung verpflichtet ist; soweit der Auftragnehmer gesetzlich zur ffenbarung verpflichtet ist, insbesondere gegenüber Aufsichtsbehörden oder berufsständischen Kammern, oder



EBERTZ DATENSCHUTZ GmbH | Ober den Wiesen 17 | 35756 Mittenaar | Amtsgericht Wetzlar HRB 8970
Geschäftsführer: Inge Ebertz und Lars Ebertz, Diplom-Ingenieur | E-Mail: info@ebertz-datenschutz.de | www.ebertz-datenschutz.de

- soweit der Auftragnehmer in seiner Eigenschaft als betrieblicher Datenschutzbeauftragter insbesondere gemäß Art. 39 Abs. 1 lit. d) und e) DSGVO zur Kooperation mit der Aufsichtsbehörde berechtigt oder verpflichtet ist.

(4) Diese Verschwiegenheitspflicht der EBERTZ DATENSCHUTZ besteht über die Dauer des Vertragsverhältnisses fort.

(5) Dieser Vertrag und sein Inhalt unterliegen wechselseitig einer über das Vertragsende hinausgehenden Verschwiegenheitsverpflichtung.

(6) Mitarbeiter und weitere Erfüllungsgehilfen sind im gleichen Umfang wie die Parteien selbst zur Verschwiegenheit zu verpflichten. Die Parteien weisen dies auf Anfrage wechselseitig nach.

**§ 12 Anwendbares Recht, Gerichtsstand, Teilnichtigkeit**

(1) Für diese Geschäftsbedingungen und die gesamten Rechtsbeziehungen zwischen der EBERTZ DATENSCHUTZ und dem Kunden gilt das Recht der Bundesrepublik Deutschland. Die Anwendung des UN-Kaufrechts wird hiermit ausdrücklich ausgeschlossen.

(2) Soweit der Kunde Vollkaufmann i. S. des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, ist der Sitz der EBERTZ DATENSCHUTZ ausschließlicher Gerichtsstand für alle sich aus dem Vertragsverhältnis unmittelbar oder mittelbar ergebenden Streitigkeiten.

(3) Sollte eine Bestimmung in diesen Geschäftsbedingungen oder eine Bestimmung im Rahmen sonstiger Vereinbarungen unwirksam sein oder werden, so wird hiervon die Wirksamkeit aller sonstigen Bestimmungen oder Vereinbarungen nicht berührt.



EBERTZ DATENSCHUTZ GmbH | Ober den Wiesen 17 | 35756 Mittenaar | Amtsgericht Wetzlar HRB 8970
Geschäftsführer: Inge Ebertz und Lars Ebertz, Diplom-Ingenieur | E-Mail: info@ebertz-datenschutz.de | www.ebertz-datenschutz.de

**ANLAGE 1**
**Vereinbarung zur Auftragsverarbeitung für die unter §1 aufgeführten Leistungen**

## 1. Gegenstand und Dauer des Vertrags

### (1) Gegenstand

Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer (Nichtzutreffendes optional streichen):

- Bereitstellung eines Datenschutzmanagement Systems (Robin Data)
- Ggfs Bereitstellung einer elearning Plattform zur Mitarbeiter Sensibilisierung (Coursepath)
- Ggfs Bereitstellung eines Whistleblowing Case Management Systems (Whistleblowing Software)

(2) Dauer

- Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit des Geschäftsbesorgungsvertrages oder der Bestellung als ext. Datenschutzbeauftragter oder der vereinbarten Bereitstellung.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).
(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

## 2. Konkretisierung des Vertragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers ist in Anlage 3 (Darstellung der Auftragsdatenverarbeitung (AV) mit dem jeweiligen Subunternehmen) aufgeführt.

### (2) Art der Daten

- Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung und in Anlage 3 – im jeweiligen AV des Subunternehmers - konkret beschrieben.

### (3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

  ☐ Beschäftigte

  ☐ Ehemalige Beschäftigte

  ☐ Mit dem Auftraggeber in Verbindung stehenden Personen
  - Kontakte von Lieferanten
  - Kontakte von Kunden
  - Kontakte von Interessenten

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.
(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.
(4) Die umgesetzten technischen und organisatorischen Maßnahmen je Leistungsmodul sind in Anlage 3 – im jeweiligen AV des Subunternehmers – umfassend beschrieben.

## 4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.
g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

**6. Unterauftragsverhältnisse**

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber mit Anlage 3 dieses AVs vorgelegt.

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.



EBERTZ DATENSCHUTZ GmbH | Ober den Wiesen 17 | 35756 Mittenaar | Amtsgericht Wetzlar HRB 8970
Geschäftsführer: Inge Ebertz und Lars Ebertz, Diplom-Ingenieur | E-Mail: info@ebertz-datenschutz.de | www.ebertz-datenschutz.de

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

### *7.* Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

- Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.
- Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

### 8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

### *9.* Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.
(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

### 10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.



EBERTZ DATENSCHUTZ GmbH | Ober den Wiesen 17 | 35756 Mittenaar | Amtsgericht Wetzlar HRB 8970
Geschäftsführer: Inge Ebertz und Lars Ebertz, Diplom-Ingenieur | E-Mail: info@ebertz-datenschutz.de | www.ebertz-datenschutz.de

## Anlage 2 - Technisch-organisatorische Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen.
Die technischen und organisatorischen Maßnahmen (TOMs) des jeweiligen Leistungsmoduls richten sich nach den dokumentierten TOMs der in Anlage 2 aufgeführten Unterauftragnehmer. Die jeweiligen Maßnahmen werden in Anlage 3 im Rahmen der Offenlegung der AVVs mit den Unterauftragnehmern zur Prüfung offengelegt.

## Anlage 3 - Genehmigte Unterauftragsverhältnisse

| Unterauftragnehmer | Anschrift/Land | Leistung | AVV / DPA |
|---|---|---|---|
| Coursepath | Fellow Digitals GmbH<br>Brüsseler Str. 25<br>50674 Köln | Bereitstellung elearning Plattform<br>https://ebertz-datenschutz.coursepath.com | AVV abgeschlossen siehe Link zum Dokument |
| Robin Data | Robin Data GmbH<br>Fritz-Haber-Str. 2<br>06217 Merseburg | Bereitstellung Secureapp Datenschutz Management System (DSMS)<br>https://secureapp.robin-data.io | AVV abgeschlossen siehe Link zum Dokument |
| Whistleblower Software | Whistleblower Software ApS<br>Inge Lehmanns Gade 105<br>8000 Aarhus C<br>Denmark | Bereitstellung Whistlebower Case Management Portal<br>https://whistleblowersoftware.com/ | AVV abgeschlossen siehe Link zum Dokument |