Auftragsverarbeitungsvertrag gemäß Artikel 28 Absatz 3 Europäischen Datenschutz-Grundverordnung (DS-GVO)

zwischen

der Hochschule
Anschrift, PLZ, Ort

− Verantwortlicher −

und

dem Verein zu Pflege und Weiterentwicklung des Arbeits- Gesundheits- und Umweltschutzmanagements e.V (AGUM e.V.), Samansstraße 13, 53227 Bonn

− Auftragsverarbeiter –

Muster

ABSCHNITT I ... 3
Klausel 1 Zweck und Anwendungsbereich ... 3
Klausel 2 Unabänderbarkeit der Klauseln ... 3
Klausel 3 Auslegung ... 3
Klausel 4 Vorrang ... 4
Klausel 5 Kopplungsklausel ... 4
ABSCHNITT II PFLICHTEN DER PARTEIEN ... 4
Klausel 6 Beschreibung der Verarbeitung ... 4
Klausel 7 Pflichten der Parteien ... 4
7.1. Weisungen ... 4
7.2. Zweckbindung ... 4
7.3. Dauer der Verarbeitung personenbezogener Daten ... 5
7.4. Sicherheit der Verarbeitung ... 5
7.5. Sensible Daten ... 5
7.6. Dokumentation und Einhaltung der Klauseln ... 5
7.7. Einsatz von Unterauftragsverarbeitern ... 6
7.8. Internationale Datenübermittlungen ... 7
Klausel 8 Unterstützung des Verantwortlichen ... 7
Klausel 9 Meldung von Verletzungen des Schutzes personenbezogener Daten ... 8
9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten ... 8
9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten ... 9
ABSCHNITT III SCHLUSSBESTIMMUNGEN ... 9
Klausel 10 Verstöße gegen die Klauseln und Beendigung des Vertrags ... 9
ABSCHNITT IV ERGÄNZENDE VEREINBARUNGEN ... 11
Klausel 11 Konkretisierungen und ergänzende Regelungen ... 11
11.1 Pflichten der Parteien ... 11
11.2 Unterstützung des Verantwortlichen ... 12
11.3 Meldung von Verletzungen des Schutzes personenbezogener Daten ... 12
11.4 Fernwartung ... 13
11.5 Sonstiges ... 14
ANHANG I Liste der Parteien ... 14
ANHANG II Beschreibung der Verarbeitung ... 16
ANHANG III Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten ... 18
ANHANG IV Liste der Unterauftragsverarbeiter ... 23

Muster

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.

Muster

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.

Muster

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

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

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

c) 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.

Muster

d) 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.

e) 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 darf keinen seiner Verarbeitungsvorgänge, die er im Auftrag des Verantwortlichen gemäß diesen Klauseln durchführt, ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen an einen Unterauftragsverarbeiter untervergeben. Der Auftragsverarbeiter reicht den Antrag auf die gesonderte Genehmigung mindestens 14 Tage vor der Beauftragung des betreffenden Unterauftragsverarbeiters zusammen mit den Informationen ein, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden. Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter findet sich in Anhang IV. Die Parteien halten Anhang IV jeweils auf dem neuesten Stand.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 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 seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Muster

7.8. Internationale Datenübermittlungen

a) 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.

b) 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].

Muster

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.

Muster

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) 2016/679 679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

Muster

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.

Muster

ABSCHNITT IV ERGÄNZENDE VEREINBARUNGEN

Klausel 11 Konkretisierungen und ergänzende Regelungen

11.1 Pflichten der Parteien

a) Weisungen

Ergänzend zu Klausel 7.1 Buchstabe a) wird vereinbart:

Die Weisungen sind von den Vertragsparteien für die Geltungsdauer der Verarbeitung und anschließend noch für drei volle Kalenderjahre aufzubewahren.

b) Sicherheit der Verarbeitung

1) Ergänzend zu Klausel 7.4 Buchstabe a) wird vereinbart:

i) Die in Anhang III vereinbarten technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Änderungen und Ergänzungen der vereinbarten technischen und organisatorischen Maßnahmen bedürfen einer schriftlichen Mitteilung an den Verantwortlichen und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Maßnahmen handelt. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen bedürfen der Zustimmung des Verantwortlichen. Bei allen Änderungen der technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter darf das Sicherheitsniveau der vereinbarten Maßnahmen nicht unterschritten werden.

ii) Bei Vergabefahren stellt der Auftragsverarbeiter dem Verantwortlichen bereits im Rahmen des Vergabeverfahrens zusammen mit seinem Angebot ein aussagekräftiges, prüffähiges und aktuelles Datenschutz- und Datensicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

iii) Der Auftragsverarbeiter verarbeitet personenbezogene Daten (auch) in Mobiler Arbeit. Der Auftragsverarbeiter hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei „Mobiler Arbeiten“ der Beschäftigten des Auftragsverarbeiters gewährleistet ist. Der Auftragsverarbeiter trägt Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten außerhalb der Geschäftsräume die Speicherorte so konfiguriert werden, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt. Der Auftragsverarbeiter trägt ferner dafür Sorge, dass die Bedingungen zum „Mobilen Arbeiten“ des Auftragsverarbeiters einschließlich spezieller Verhaltens- und IT-Sicherheitsrichtlinien, von den jeweiligen Beschäftigten eingehalten werden; die jeweiligen Beschäftigten werden hinsichtlich der Einhaltung datenschutzrechtlicher Anforderungen durch den Auftragsverarbeiter in geeigneter Weise geschult.

2) Ergänzend zu Klausel 7.4 Buchstabe b) wird vereinbart:

Die Pflicht zu Vertraulichkeit/Verschwiegenheit dieser Personen besteht auch nach Beendigung dieses Vertrages und/oder des Beschäftigungsverhältnisses zwischen dem Auftragsverarbeiter und den bei ihm Beschäftigten fort.

Muster

c) Dokumentation und Einhaltung der Klauseln

Ergänzend zu Klausel 7.6 Buchstabe a) wird vereinbart:

Der Auftragsverarbeiter unterstützt den Verantwortlichen auf dessen Verlangen bei der Erstellung und Führung des Verzeichnisses über die Verarbeitungstätigkeiten, insbesondere durch Mitteilung der erforderlichen Angaben.

d) Einsatz von Unterauftragsnehmern

Ergänzend zu Klausel 7.7 Buchstabe a) wird vereinbart:

Die Liste der bestehenden Unterauftragsverarbeiter wird dem Verantwortlichen vor Vertragsschluss zur Verfügung gestellt.

Ergänzend zu Klausel 7.7 Buchstabe b) wird vereinbart:

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 Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

11.2 Unterstützung des Verantwortlichen

Ergänzend zu Klausel 8 Buchstabe a) wird vereinbart:

Der Auftragsverarbeiter darf Auskünfte an Dritte oder betroffene Personen nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Ist der Auftragsverarbeiter gerichtlich oder gesetzlich verpflichtet, Auskunft zu erteilen, so hat er den Verantwortlichen hierüber unverzüglich zu informieren. Der Auftragsverarbeiter darf Auskünfte an den Verantwortlichen nur gegenüber den autorisierten Personen (gemäß Anhang I) erteilen.

Ergänzend zu Klausel 10 Buchstabe d) wird vereinbart:

Ein Zurückbehaltungsrecht wird hinsichtlich der verarbeiteten personenbezogenen Daten und der zugehörigen Datenträger ausgeschlossen.

11.3 Meldung von Verletzungen des Schutzes personenbezogener Daten

Ergänzend zu Klausel 9.2 wird vereinbart:

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, Verdacht auf Verletzung des Schutzes personenbezogener Daten, anderen Unregelmäßigkeiten bei der Datenverarbeitung außerdem unverzüglich, bei Kontrollhandlungen und Maßnahmen einer Aufsichts- oder Ermittlungsbehörde. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn die bei ihm getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht (mehr) genügt.

Muster

11.4 Fernwartung (trifft nicht zu)

a) Der Auftragsverarbeiter darf im Rahmen der Fernwartung nur auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Fernwartung erforderlich ist. Ferner ist dem Auftragsverarbeiter bei der Fernwartung untersagt, personenbezogene Daten des Verantwortlichen auf eigenen IT-Systemen bzw. Datenträgern zu speichern, es sei denn der Verantwortliche weist ihn hierzu an. Der Verantwortliche wird dem Auftragsverarbeiter nur die für die Durchführung der vereinbarten Tätigkeiten benötigten Zugriffsrechte bereitstellen, deren Aktualität regelmäßig überprüfen und gegebenenfalls Korrekturen vornehmen. Der Auftragsverarbeiter darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Tätigkeiten unerlässlichen Umfang Gebrauch machen.

b) Der Auftragsverarbeiter hat dem Verantwortlichen Fernwartungsarbeiten im Vorfeld anzukündigen. Der Verantwortliche ist berechtigt, die Durchführung der Fernwartung mit zu verfolgen bzw. Aufzeichnungen (z. B. Screenrecording, Screenshots o. Ä.) von dieser zu erstellen. Auf Anfrage und soweit erforderlich, wirkt der Auftragsverarbeiter an der Konfiguration technischer Kontrolleinrichtungen mit.

c) Der Verantwortliche hat das Recht, den Zugriff des Auftragsverarbeiters auf die informationstechnischen Systeme des Verantwortlichen zu unterbrechen. Dies gilt insbesondere, wenn der Verdacht besteht, dass unbefugt auf Informationen und Ressourcen zugegriffen wird.

d) Im Rahmen der beauftragten und zu leistenden Fernwartungsarbeiten hat der Auftragsverarbeiter folgende Rahmenbedingungen bei Zugriff auf das Netzwerk, die IT-Systeme und Anwendungen des Verantwortlichen zu beachten:

- Der Auftragsverarbeiter erhält für Arbeiten an den IT-Systemen und Anwendungen personalisierte Benutzerkennungen. Jeder Mitarbeiter des Auftragsverarbeiters erhält eine eigene personalisierte Benutzerkennung. Der Auftragsverarbeiter nutzt die ihm überlassenen personalisierten Benutzerkennungen ausschließlich für die beauftragten Tätigkeiten und gibt diese nicht an Dritte weiter. Die Kennwortrichtlinien des Verantwortlichen sind einzuhalten.
- Nutzt der Auftragsverarbeiter für die Ausübung seiner Tätigkeiten eigene technische Geräte stellt er durch adäquate und dem Stand der Technik entsprechende, angemessene Maßnahmen sicher, dass von diesen keine Gefahren für die Netzinfrastruktur, IT-Systeme und Anwendungen des Verantwortlichen ausgehen.
- Änderungen an den IT-Systemen und Anwendungen seitens des Auftragsverarbeiters sind mit dem Verantwortlichen abzustimmen und in einem adäquaten, prüffähigen Umfang zu dokumentieren.

e) Insbesondere beim Fernzugriff auf das Netzwerk und die IT-Systeme des Verantwortlichen gelten die zusätzlichen Bedingungen:

- Das Netz und die für die Fernwartung genutzten IT-Systeme des Auftragsverarbeiters müssen adäquat gegen unberechtigte Zugriffe geschützt sein.
- Der Fernzugriff auf das Netzwerk des Verantwortlichen erfolgt ausschließlich über eine nach dem Stand der Technik angemessen sichere, verschlüsselte Verbindung.
- Der Fernzugriff sollte generell nur innerhalb der üblichen Arbeitszeiten des Verantwortlichen durchgeführt werden. Ein Fernzugriff außerhalb dieser Zeiten ist mit dem Verantwortlichen abzustimmen und zu dokumentieren.
- Der Zugriff ist nach erfolgter Tätigkeit zu beenden und die Verbindung zu schließen.

Muster

- Die erfolgten Zugriffe werden vom Auftragsverarbeiter wie folgt protokolliert und zur Verfügung gestellt.
- Für jeden Fernzugriff werden von der ausführenden Person des Auftragsverarbeiters die folgenden Angaben in die Protokolldatei des Auftragsverarbeiters eingetragen:
    a) Datum/Uhrzeit der Anmeldung
    b) Dauer
    c) Name der ausführenden Person
    d) Zweck der Anmeldung (bspw. Einspielen des Patches <…>, Fehlersuche nach Incident <…>, …)

11.5 Sonstiges

a) Die Haftung bemisst sich nach den Regelungen des Artikel 82 DS-GVO. Im Übrigen gelten für die Haftung die Regelungen des dieser Vereinbarung zugrundeliegenden Vertragsverhältnisses.

b) Änderungen, Ergänzungen und Nebenabreden dieses Vertrages sind schriftlich zu vereinbaren, was auch in einem elektronischen Format erfolgen kann.

c) Sollten in diesen Vereinbarungen eine oder mehrere Bestimmungen unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Vertragsbestimmungen hierdurch nicht berührt. Die Vertragspartner werden die unwirksame oder undurchführbare Bestimmung durch eine Bestimmung ersetzen, die deren Sinn und Zweck am nächsten kommt. Gleiches gilt für den Fall einer ungewollten Regelungslücke.

Verantwortlicher

Ort und Datum	Name in Druckbuchstaben	Unterschrift

Auftragsverarbeiter

Bonn,	Anja Jubelius	Anja Jubelius
Ort und Datum	Name in Druckbuchstaben	Unterschrift

Muster

ANHANG I Liste der Parteien

1. Verantwortliche(r):

Name: Hochschule XXX

Anschrift: XXX

Datenschutzbeauftragter:

Name: ……..

Kontaktdaten: ……..

Name, Funktion und Kontaktdaten der Kontaktperson:

Weisungsberechtigt auf Seiten des Verantwortlichen ist:

Name: ……..

Telefon: ……..

E-Mail: ……..

(ggfs. Funktion, ggfs. Organisationseinheit): ……..

2. Auftragsverarbeiter:

Verein zur Pflege und Weiterentwicklung des Arbeits-, Gesundheits- und Umweltschutzmanagements e. V. (AGUM e.V.)
Samansstraße 13
53227 Bonn

Ansprechpartner für den Datenschutz:

Name: Anja Jubelius
E-Mail: jubelius@agu-management.de

Weisungsempfänger auf Seiten des Auftragsverarbeiters ist:

Name: Anja Jubelius
Telefon: 0228 36036235
Handy: 0157 34807612
E-Mail: jubelius@agu-management.de

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner*innen sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch Nachfolger*innen bzw. Vertreter*innen mitsamt Kontaktdaten mitzuteilen.

Muster

ANHANG II Beschreibung der Verarbeitung

Der Verantwortliche entscheidet darüber, welche Art von personenbezogenen Daten zu welchen Kategorien betroffener Personen der Verantwortliche vom Auftragsverarbeiter verarbeiten lässt.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

☐ Studierende

☐ Studienbewerber*innen

☐ Beschäftigte

☐ Geschäftspartner*innen

☐ Proband*innen

☐ Sonstige Kategorien betroffener Personen:

……..…

……..…

Kategorien personenbezogener Daten, die verarbeitet werden:

☐ Namen

☐ Adressdaten

☐ Kontaktdaten

☐ Funktionen

☐ Fotos

☐ Sonstige Kategorien personenbezogener Daten

……..…

……..…

Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen

☐ ……

☐ Es werden keine sensiblen Daten verarbeitet

Muster

Art der Verarbeitung:

Der Auftragsverarbeiter erfasst, organisiert und speichert personenbezogene Daten und stellt diese in dem vom Verantwortlichen zur Verfügung gestellten AGU-Managementsystem bereit. Zudem werden personenbezogene Daten nach Beendigung des Vertrags gelöscht bzw. vernichtet.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten zum Zwecke der Erfüllung seiner satzungsmäßigen Verpflichtungen im Rahmen der Zurverfügungstellung des AGU-Managementsystems als webbasiertes Managementhandbuch für den Verantwortlichen sowie zum Zwecke der Unterstützung des Verantwortlichen bei der Nutzung des Systems.

Dauer der Verarbeitung

Die Dauer der Verarbeitung richtet sich nach der Laufzeit der satzungsmäßigen Verpflichtungen des Auftragsverarbeiters gegenüber dem Verantwortlichen.

Die Verarbeitung kann über die Laufzeit hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Verantwortlichen andauern.

Drittlandtransfer

Die Erbringung der vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

Muster

ANHANG III Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit gemäß Art. 32 DS-GVO.

Die Daten werden auf Servern der Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, gehostet. Insoweit wird ausdrücklich auch auf die mitgeltenden technischen und organisatorischen Maßnahmen der Hetzner Online GmbH verwiesen. Eine Übermittlung personenbezogener Daten in Drittländer außerhalb der Europäischen Union findet nicht statt.

1. Vertraulichkeit

Zutrittskontrolle

Sicherungsmaßnahmen des Gebäudes sowie innerhalb des Gebäudes und der Geschäftsräume und besonders sensibler Räume (Geschäftsleitung, Personalabteilung, IT etc.). Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocatino Rack)
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Abschließbare Büroräume
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen

Zugangskontrolle

Zugang zu Datenverarbeitungsanlagen auf Netz- und Serverebene; Die Zugangskontrolle soll sicherstellen, dass nur berechtigte Personen oder Computer Zugang zur IT erhalten. Zentrale Elemente sind die Identifikation und die Authentifikation. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- (Verschlüsselte) Identifikation und Authentifikation von Benutzern (User-ID und Passwort, Zweistufenauthentifizierung mit Magnet-/Chipkarte oder Token, biometrisches Verfahren etc.)
- Passwortregeln vorhanden (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss von Trivialkennworten etc.)

Muster

- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Sperrung bei wiederholter Fehleingabe von Passwörtern
- Freigabe nur durch Administrator/Freigabe nach Zeitablauf/Freigabe gestaffelt nach Versuchen
- Alarmierung bei Überschreitung definierter Grenzwerte an fehlerhaften Anmeldeversuchen
- Zugang ins Internet mit Administrationsrechten nicht möglich
- Hardware-Firewall/Software-Firewall vorhanden
- Updates für Firewall werden regelmäßig automatisch/manuell installiert
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Protokollierung von Internetnutzung
- Regelmäßige Sicherheitsupdates

Zugriffskontrolle

Maßnahmen zur Steuerung und Überwachung des Zugriffs auf Datenverarbeitungssysteme. Die Zugriffskontrolle soll sicherstellen, dass nur die zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen, insbesondere nach „Lesen, Schreiben, Ausführen“
- Rollen- und Rechtekonzept mit einer Festlegung und Dokumentation der Rollen und Rechte der berechtigten Personen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte
- Regelmäßige Überprüfung der Erforderlichkeit der vergebenen Rollen und Rechte
- Kein Zugriff durch Benutzer auf Systemebene möglich

Trennungskontrolle

Maßnahmen, die sicherstellen sollen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Logische/physikalische Trennung von verschiedenen speichernden Stellen (Unternehmen)
- Trennung unabhängiger Anwendungen innerhalb eines Unternehmens (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung von Test- und Produktionsdaten (getrennte Programmbibliotheken etc.)

Muster

- Trennung der DV-Anlagen und Datenträger für besonders sensible Daten (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung nach Zwecken (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)

Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Sensible Daten/Dokumente werden nach Möglichkeit anonymisiert/pseudonymisiert übertragen/weitergegeben

2. Integrität

Weitergabekontrolle

Maßnahmen, um sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Sensible Daten/Dokumente werden verschlüsselt/anonymisiert/pseudonymisiert übertragen/weitergegeben
- Identifizierung und Authentifizierung der Beteiligten bei der Datenübertragung (Benutzerkennung/Passwort etc.)
- Einsatz von E-Mail-Contentfiltern
- Sichere und vertrauliche Sammlung von Datenträgern/Unterlagen vor der Vernichtung (verschlossene Sammelbehälter etc.)
- Regelmäßige datenschutzgerechte Löschung/Vernichtung von Datenträgern/Unterlagen, deren Aufbewahrungspflicht abgelaufen ist
- Einsatz von Aktenvernichtern

Muster

Eingabekontrolle

Maßnahmen, um sicherzustellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert, kopiert oder gelöscht wurden. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Protokollierung der Einrichtung/Änderung von Benutzern und Rechten (Dokumentation aller berechtigten Nutzer, Rechteprofile der berechtigten Nutzer, Dokumentation von Änderungen von Nutzern/Rechten, Dokumentation, wer die Benutzer und Rechte angeordnet/eingerichtet hat, Historie über die eingerichteten Nutzer und Rechte etc.)
- Protokollierung von Systemänderungen (Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfälle, Testung, Testergebnisse und Freigabe, Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)
- Protokollierung von Eingaben und Veränderungen (Datum und Uhrzeit von Zugriffen mit Kennung des Benutzers, Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge, Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten, unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)
- Systemüberwachung (Protokollierung von benutzten Programmen, Systemstart und -stopp, Anmeldung/Abmeldung von Benutzern, Anmelde-Fehlversuche, Anschluss und Entfernung von Ein- und Ausgabegeräten, Aktivitäten im Zusammenhang mit Fremdwartung und Fernwartung, Systemwarnungen oder Systemfehler, Konsolwarnungen und Konsolmeldungen, am Paketfilter wegen Regelverstoß abgewiesene Pakete, Änderungen und Änderungsversuche von Gateway- und Firewallpolicies, Systemprotokollausnahmen, Zugriffe auf die Server-Registry, Konfigurations- und Statusänderungen, Systemfehler, Regelverstöße, Maßnahmen zur System- und Datenwiederherstellung, wie Restore- und Back-up-Maßnahmen, Änderungen von Konfigurationseinstellungen etc.)
- Gewährleistung der Sicherheit von Protokolldateien (Kein Abschalten der Protokollfunktionen möglich, kein Bearbeiten/Löschen der Protokolldateien möglich, Protokollierung der Abschaltung von Protokollfunktionen, Protokollierung der Bearbeitung/Löschung von Protokolldateien, Protokollierung von Zugriffen auf die Protokolldateien, verschlüsselte Speicherung der Protokolldateien etc.)

Muster

3. Verfügbarkeit und Belastbarkeit

Maßnahmen, um sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden. Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Ausfallschutz durch gespiegelte Plattenlaufwerke, RAID-System etc.
- Backup-Konzept
- Regelmäßige automatisierte/manuelle Datensicherungen
- Sichere Übertragung/Transport von Datensicherungen/Sicherungsdatenträgern
- Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit
- Überwachung der Sicherungsdatenträger bezüglich ihrer Haltbarkeit/Anzahl der zulässigen Schreibzyklen
- Recovery-Konzept
- Prüfung der Rekonstruierbarkeit der Datenbestände durch regelmäßige Tests
- Administratorenpasswort/Notfallpassworte sicher hinterlegt (Tresor, Bankschließfach etc.)
- Schriftliches Administrationskonzept
- Vier-Augen-Prinzip bei sensiblen Administratortätigkeiten
- Test- oder Entwicklungsumgebung vorhanden (Tests mit anonymisierten Echtdaten)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Datenschutz-Maßnahmen

Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Benennung eines Datenschutzbeauftragten/Ansprechpartners für den Datenschutz
- Verpflichtung der Mitarbeiter zur Vertraulichkeit
- Datenschutzfreundliche Voreinstellungen: Es werden nicht mehr personenbezogene Daten erhoben als für den Zweck erforderlich

Muster

Auftragskontrolle (Outsourcing an Dritte)

Der Auftragsverarbeiter trifft die folgenden Maßnahmen:

- Vorherige Prüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen; Vertraglich festgelegte Verantwortlichkeiten; Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit etc.
- Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien

ANHANG IV Liste der Unterauftragsverarbeiter

Hoster/Provider:

Name:	Hetzner Online GmbH
Anschrift:	Industriestr. 25 91710 Gunzenhausen Deutschland
Zweck/Gegenstand:	Hoster/Provider
Dauer:	Die Dauer der Verarbeitung richtet sich nach der Laufzeit der Bereitstellung und Nutzung des AGUM-Systems. Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Verantwortlichen andauern.

E-Mail-Server:

Name:	Domainfactory GmbH
Anschrift:	c/o WeWork Neuturmstrasse 5 80331 München Deutschland
Zweck/Gegenstand:	E-Mail-Server
Dauer:	Die Dauer der Verarbeitung richtet sich nach der Laufzeit der Bereitstellung und Nutzung des AGUM-Systems. Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Verantwortlichen andauern.

Muster