

Auftragsverarbeitungsvereinbarung innerhalb der EU/EWR

1. Die in **Anhang I** aufgeführten Parteien schließen zum Schutz personenbezogener Daten und zur Einhaltung der Art. 28 Abs. 3 und 4 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung – DSGVO) diese Auftragsverarbeitungsvereinbarung.
2. Die folgenden Anlagen und Anhänge sind wesentlicher Bestandteil dieser Auftragsverarbeitungsvereinbarung:
 - Anlage:** **Standardvertragsklauseln** zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 (7) der Verordnung (EU) 2016/679 gemäß Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 („Standardvertragsklauseln“)
 - Anhang I:** Liste der **Parteien**
 - Anhang II:** **Beschreibung der Verarbeitung**
 - Anhang III:** **Technische und organisatorische Maßnahmen**, einschließlich zur Gewährleistung der Sicherheit der Daten
 - Anhang IV:** Liste der **Unterauftragsverarbeiter**
3. In Ergänzung und sofern die nachfolgenden Regelungen weder unmittelbar noch mittelbar den Standardvertragsklauseln widersprechen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden, vereinbaren die Parteien Folgendes:
4. Diese Auftragsverarbeitungsvereinbarung tritt an die Stelle und ersetzt alle früheren Auftragsverarbeitungsvereinbarungen zwischen den Parteien.
5. 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.
6. Diese Auftragsverarbeitungsvereinbarung unterliegt deutschem Recht. Für alle Streitigkeiten, die sich aus dieser Auftragsverarbeitungsvereinbarung ergeben, ist Gerichtsstand Böblingen, Deutschland.

Anlage:

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 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 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 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 – fakultativ

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 personenbezogener 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 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.
- 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 besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens Vierzehn (14) Tage 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 betreffenden 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 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 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.

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 [OPTION 1: Artikel 32 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725].
- 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 [OPTION 1: Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725] 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 [OPTION 1: Artikel 34 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 35 der Verordnung (EU) 2018/1725], 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 [OPTION 1: Artikel 33

und 34 der Verordnung (EU) 2016/679] oder [OPTION 2: Artikel 34 und 35 der Verordnung (EU) 2018/1725] 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 – 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 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 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.

ANHANG 1: LISTE DER PARTEIEN

Verantwortliche(r): [Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen]	
Firmierung/Name	
Anschrift	
Name, Funktion und Kontaktdaten der Kontaktperson	
Ggf. Kontaktdaten des Datenschutzbeauftragten	
Datum des Vertragbeitritts	
Unterzeichnung	

Auftragsverarbeiter: [Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters]	
Firmierung/Name	1cc GmbH
Anschrift	Max-Eyth-Str. 35, 71088 Holzgerlingen
Name, Funktion und Kontaktdaten der Kontaktperson	Sebastian Hotz, Geschäftsführer E-Mail: info@1cc-consulting.com
Ggf. Kontaktdaten des Datenschutzbeauftragten	Michael Weinmann E-Mail: michael.weinmann@dsb-office.de , Tel.: 0173-7632962
Datum des Vertragbeitritts	
Unterzeichnung	

ANHANG 2: BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Nutzer der Compliance-Management-Plattform
- Personen, deren Legitimationsdaten gespeichert für Meldungen gespeichert werden, Insbesondere Leiter der Verantwortlichen Stelle

Kategorien personenbezogener Daten, die verarbeitet werden

- Angaben zu den Personen, welche Inhalt der Meldungen sind (insbesondere Leiter der Verantwortlichen Stelle)
- Daten zu Nutzern der Compliance-Management-Plattform wie Name, Benutzername, Berechtigungen, Daten zur Authentifizierung.
- Daten zur Nutzung der Compliance-Management-Plattform (Log-Files, Aktionen im Zusammenhang mit der Nutzung wie Eingaben von Informationen, IP-Adressen im Zusammenhang mit dem Aufruf des Web-Service, Zeitstempel der Nutzung)

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

- Nicht relevant

Art der Verarbeitung

- Im Rahmen der Compliance-Management-Plattform sind alle Arten der Verarbeitung gem. Art. 4 Nr. 2 relevant. Insbesondere das Erheben von Informationen zur für die Meldung verantwortliche Stelle und der Inhalte von Meldungen, die Speicherung der Informationen und das Übermitteln an die jeweilige Registrierungsbehörde

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

- Durchführung der Meldungen zur Erfüllung der gesetzlichen Umwelt-Compliance Anforderungen.

Dauer der Verarbeitung

- Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung
- Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben.

ANHANG 3: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel (z. B. Schlüsselbuch)
- Schließsystem - Einsatz eines Schließsystems
- Regelung zum Umgang mit Besuchern - Besucher werden empfangen und begleitet.
- Sicherheitszonen mit eigenständigen Zutrittsregelungen - Definition von Sicherheitszonen, beispielsweise Serverräume, mit eigenständiger Zutrittsregelung.

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifizierung mit Benutzername und Passwort - Authentifizierung mit Benutzername und Passwort
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitsdienst
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit modernen Methoden
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerks

M.1.3 Beschreibung der Zugriffskontrolle:

- Autorisierungskonzept - Erstellung und Nutzung eines Autorisierungskonzepts
- Datenlöschung - Sichere Löschung von Datenträgern vor der Wiederverwendung (z. B. durch mehrfaches Überschreiben)
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit modernen Methoden
- Verschlüsselung von Smartphones - Verschlüsselung von Smartphones mit modernen Methoden
- Passwortrichtlinie - Passwortrichtlinie, einschließlich Länge, Komplexität und Häufigkeit des Wechsels
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern
- Trennung Genehmigung u. Einrichtung von Berechtigungen - Rechte zur Einräumung von Rechten ist getrennt von Personen, welche Rechte administrativ einrichten.

M.1.4 Beschreibung der Weitergabekontrolle:

- SSL/TLS-Verschlüsselung - Nutzung von SSL/TLS-Verschlüsselung bei der Übertragung von Daten im Internet
- VPN-Tunnel - Einrichtung von VPN-Tunneln für den externen Zugriff auf das Netzwerk

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (auf Softwareseite)
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem

M.1.6 Beschreibung der Verschlüsselung:

- Mobile Systeme werden verschlüsselt - Mobile Geräte (Beispielsweise Notebooks, Tablets, Phones, USB-Sticks) werden nach Stand der Technik verschlüsselt.
- Übertragung - Verschlüsselte Übertragung von Daten (z. B. E-Mail-Verschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Verwendung des FTAPI-Datentransfertools)

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Zugriffsrechte - Persönliche Zugriffsrechte zur Nachverfolgung von Zugriffen
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten
- Personalisierte Benutzernamen - Nachverfolgbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Klimaanlage - Klimaanlage in Serverräumen
- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Backup- und Wiederherstellungskonzept - Erstellung eines Backup- und Wiederherstellungskonzepts
- Notfall-IT-Plan - Erstellung und Anwendung von Notfall-IT-Plänen
- Feuerlöscher - CO2-Feuerlöscher in Serverräumen
- Ausgelagerte Datensicherung - Speicherung der Datensicherung an einem sicheren, externen Ort
- Redundante Datenspeicherung - Redundante Datenspeicherung (z. B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Unterbrechungsfreie Stromversorgung - (USV) unterbrechungsfreie Stromversorgung

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Aktivitäten
- Auftragsverarbeitung - Abschluss eines Auftragsvertrags gemäß Art. 28 DSGVO
- Auswahl - Auswahl des Auftragnehmers aus der Perspektive der gebotenen Sorgfalt (insbesondere in Bezug auf Datenschutz)

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Benennung eines Datenschutzbeauftragten - Es ist ein Beauftragter für den Datenschutz benannt und bei der Aufsichtsbehörde gemeldet
- Datenschutzmanagementsystem - Managementsystem zum Schutz von Daten (z. B. basierend auf ISO 27701)
- Softwarebasierte Werkzeuge - Einsatz von softwarebasierten Werkzeugen zur Einhaltung der Datenschutzanforderungen (z. B. audatis MANAGER)
- Schulung - Schulungen für alle autorisierten Mitarbeiter. Regelmäßige Nachschulungen.
- Verbindliche Weisung/Organisation zur Erfüllung der gesetzlichen Anforderungen - Zur Erfüllung der gesetzlichen Anforderungen wurde in betrieblichen Anweisungen (Beispielsweise Datenschutz-Richtlinie, Prozessregelungen zu Datenschutzverletzungen, Anfragen Betroffener...) verbindliche Regelungen festgehalten.

Bemerkungen zur Maßnahmenbeschreibung:

Die Server zum Betrieb der Compliance-Management Plattform werden beim Unterauftragnehmer Hetzner Online GmbH betrieben. Diesbezüglich wird ausdrücklich auf das Dokument <https://www.hetzner.com/AV/TOM.pdf> verwiesen.

ANHANG 4: LISTE DER UNTERAUFTRAGSVERARBEITER

ERLÄUTERUNG:

Dieser Anhang muss im Falle einer gesonderten Genehmigung von Unterauftragsverarbeitern ausgefüllt werden (Klausel 7.7 Buchstabe a, Option 1).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

- Hosting Web-Server:
HubSpot, Inc. Two Canal Park, MA 02141, Cambridge, USA
Garantien: Standardvertragsklauseln, Registrierung EU-U.S. DPF

- Automatisierung der Plattform
HubSpot, Inc, Two Canal Park, MA 02141, Cambridge, USA
Garantien: Standardvertragsklauseln, Registrierung EU-U.S. DPF

- Erstellung von Dokumenten und Zeichnungsprozessen
PandaDoc, Inc.; 3739 Balboa St.; #1083; CA 94121; San Francisco; USA
Garantien: Standardvertragsklauseln, Registrierung EU-U.S. DPF

- Zahlungsdienste
Stripe, Legal Process, 510, Townsend St., San Francisco, CA 94103, USA
Garantien: Standardvertragsklauseln, Registrierung EU-U.S. DPF