Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates

Standardvertragsklauseln

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

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

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

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

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

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

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

Klausel 2

Unabänderbarkeit der Klauseln

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

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

Klausel 3

Auslegung

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

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

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

Klausel 4

Vorrang

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

Klausel 5 – 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 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.

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

f) 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 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.

a) 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.

b) 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.

c) 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.

d) 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 Artikel 32 der Verordnung (EU) 2016/679.

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

Klausel 9

Meldung von Verletzungen des Schutzes personenbezogener Daten

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

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

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

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

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

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

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

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

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

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

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

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

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

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

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

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

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

ABSCHNITT III - SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

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

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

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

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

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

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

ANHANG I - LISTE DER PARTEIEN

Verantwortliche(r):

„Kunde" gemäß Rahmenvereinbarung „Einsatz der DEFENDERBOX Cybersecurity Box"

Auftragsverarbeiter:

SMB Cybersecurity GmbH

Freiherr-vom-Stein-Straße 7b

57223 Kreuztal

Markus Schulte, Geschäftsführer, Tel. 02732-7652088

ANHANG II - BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- Kundendaten
- Mitarbeiterdaten

Kategorien personenbezogener Daten, die verarbeitet werden

- Protokolldaten (z.B. Logfiles)
- Kommunikationsdaten (z.B. Mailadresse, IP-Adresse)

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 Daten gem. Art. 9 Abs. 1 DS-GVO (rassische/ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschafszugehörigkeit, genetische/biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben/sexuellen Orientierung) verarbeitet.

Art der Verarbeitung

Der Gegenstand der Verarbeitung ist in Abschnitt „4. Scope of services" der Rahmenvereinbarung beschrieben.

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

Der Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ist in der Rahmenvereinbarung konkret beschrieben

Dauer der Verarbeitung

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Rahmenvereinbarung.

ANHANG III - TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN.

1. Vertraulichkeit

1. Zutrittskontrolle – Bezieht sich auf die Standorte der Server

Der räumliche Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren.

☒ Das Unternehmen verfügt über einen zentralen und besetzten Empfangsbereich

☒ Die Räumlichkeiten des Unternehmens sind stets verschlossen

☒ Es existiert eine Zutrittsregelung für betriebsfremde Personen (z.B. Begleitung, Besucherausweis).

☒ Im Unternehmen ist eine zentrale Schlüsselverwaltung zur Ausgabe von Schlüsseln etabliert.

☒ An zentraler Stelle wird eine Schlüsselliste geführt, aus der hervorgeht, welcher Mitarbeiter wann einen Schlüssel erhalten hat.

☒ Mitarbeiter wurden schriftlich dazu verpflichtet, den Verlust eines Schlüssels umgehend zu melden.

☒ Der Zutritt zu Serverräumen ist auf berechtigte Mitarbeiter beschränkt.

☒ Serverräume sind stets verschlossen.

☒ Es erfolgt eine Protokollierung der Zutritte zu Serverräumen.

☒ Es ist eine Alarmanlage installiert.

☒ Eine Gebäudeüberwachung erfolgt durch Video, Werkschutz oder Nachtwächter/Wachdienst.

2. Zugangskontrolle

Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können.

☒ Mitarbeiter erhalten individuelle Benutzernamen und Kennwörter für die Anmeldung am PC-Arbeitsplatz.

☒ Initialkennwörter müssen vom Anwender geändert werden

☒ Kennwörter verfügen über Komplexitätsanforderungen (z.B. Zahlen, Buchstaben, Sonderzeichen).

☒ Kennwörter sind mindestens 8 Zeichen lang.

☒ Administrative Kennwörter sind mindestens 12 Zeichen lang.

☐ Kennwörter müssen regelmäßig geändert werden.

☒ Verfahren einer Zwei-Faktor-Authentifizierung befinden sich im Einsatz.

☒ PC-Arbeitsplätze werden bei Inaktivität automatisch gesperrt und können nur durch Kennworteingabe wieder entsperrt werden.

☒ Interne Netze sind gegen unberechtigte Zugriffe von extern durch eine Firewall geschützt.

☒ Externe Zugriffe auf interne Netze sind ausschließlich über verschlüsselte Verbindungen (z.B. VPN) möglich.

☒ Datenträger von mobilen Endgeräten (Notebooks, Smartphones, Tablets), auf denen sich personenbezogene Daten befinden, sind verschlüsselt.

☒ PC-Arbeitsplätze und Notebooks verfügen über einen Anti-Viren-Schutz.

3. **Zugriffskontrolle**

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒ Ein Berechtigungskonzept liegt im Unternehmen vor und enthält differenzierte Berechtigungsstufen.

☒ Benutzerkonten werden zeitnah mit Ausscheiden aus dem Arbeitsverhältnis gesperrt.

☒ Über Benutzerprofile ist in den Anwendungen sichergestellt, dass Mitarbeiter ausschließlich die Rechte erhalten, die zur Aufgabenerfüllung notwendig sind.

☒ USB-Anschlüsse an den PC-Arbeitsplätzen sind gesperrt bzw. unterliegen einer technischen Überwachung.

☒ Mitarbeiter sind dazu verpflichtet, ausschließlich vom Unternehmen ausgegebene externe Datenträger zu verwenden.

☒ Nicht mehr benötigte IT-gestützte Datenträger werden datenschutzgerecht entsorgt.

☒ Administrative Rechte stehen ausschließlich für berechtigte Mitarbeiter zur Verfügung.

4. **Trennungsgebot (Trennungskontrolle)**

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

☒ Erstellung eines Berechtigungskonzepts

☒ Mandantentrennung

☒ Trennung von Produktiv- und Testsystem

☒ Daten unterschiedlicher Projekte / Auftraggeber werden, soweit möglich, getrennt verarbeitet.

☒ Festlegung von Datenbank- und Anwendungsrechten

2. Integrität

1. **Weitergabekontrolle**

Bei einer Weitergabe personenbezogener Daten ist sicherzustellen, dass die Daten während der Übertragung oder des Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

☒ sorgfältige Auswahl von Personal und/oder Transportbehälter-/verpackung bei physischem Transport

☒ Verschlüsselung von Datenträgern bei physischem Transport

☒ Einsatz geeigneter Verschlüsselungsmethoden (z.B. VPN, https, SFTP, Inhaltsverschlüsselung von E-Mails)

☒ Transportverschlüsselung von E-Mails (TLS)

2. **Eingabekontrolle**

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten unter Verwendung

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch die Nutzer

☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

☒ Ein Datensicherungskonzept ist im Unternehmen umgesetzt.

☒ Datensicherungen werden regelmäßig durchgeführt.

☒ Datensicherungen werden regelmäßig überprüft.

☒ Datensicherungen werden an einem sicheren, ggf. externen Ort aufbewahrt.

☒ Alle PC-Systeme verfügen über aktuelle Virenschutzfunktionen

☒ Alle Server verfügen über aktuelle Virenschutzfunktionen

☒ Die Virenschutzfunktionen aktualisieren sich automatisch

☒ Betriebssysteme auf PC-Systemen werden regelmäßig aktualisiert

☒ Betriebssysteme auf Servern werden regelmäßig aktualisiert.

☒ Im Unternehmen sind Verfahren etabliert, die eine regelmäßige Aktualisierung für Hilfsprogramme (z.B. PDF-Reader, zip-Programme) gewährleisten

☒ Im Unternehmen gibt es verbindliche Richtlinien für die Wartung und Durchführung von Updates

☒ Kritische IT-Systeme im Unternehmen, insbesondere solche mit Erreichbarkeit über das Internet, werden Schwachstellentests unterzogen.

☒ Die Firewall- und Routersysteme werden regelmäßig aktualisiert (Firmwareupdate).

☒ Durch ein automatisches und permanentes Monitoring zur Erkennung von Störungen werden etwaige Fehler schnell gemeldet.

☒ Ein dokumentiertes Notfallkonzept ist im Unternehmen vorhanden.

☒ Es werden regelmäßig Notfallübungen durchgeführt.

☒ Es erfolgt eine redundante Absicherung von Servern und Datenbeständen.

☒ In Serverräumen liegt eine angemessene unterbrechungsfreie Stromversorgung (USV) vor.

☒ Die Serverräume verfügen über redundante Klimaanlagen.

☒ Im oder vor den Serverräumen befinden sich Feuerlöscheinrichtungen.

☒ Die Serverräume verfügen über einen Sensor für die Alarmanlage.

☒ Der Zutritt zu Serverräumen ist auf berechtigte Personen eingeschränkt.

4. Regelmäßige Überprüfung, Evaluierung und Bewertung

1. Datenschutzmanagement

Sicherstellung der Etablierung eines angemessenen Datenschutzmanagementsystems

☒ Ein Datenschutzbeauftragter ist schriftlich bestellt

☒ Die Mitarbeiter sind schriftlich zur Verschwiegenheit verpflichtet

☒ Datenschutz-Folgenabschätzung werden im erforderlichen Umfang durchgeführt und protokolliert

☒ Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell

☒ Ein Verzeichnis der Verarbeitungstätigkeiten liegt auch für Auftragsverarbeitungen vor und ist vollständig und aktuell

☒ Im Unternehmen bestehen schriftliche Vorgaben (z.B. Richtlinie, Betriebsvereinbarungen) für den Umgang mit Daten und den IT-Systemen.

☒ Regelmäßige Überprüfung der Sicherheit der Verarbeitung

☒ Mitarbeiterschulungen zum Datenschutz werden durchgeführt

☒ Berichterstattung durch den Datenschutzbeauftragten

☐ Im Unternehmen liegt eine Zertifizierung im Bereich der Informationssicherheit vor (z.B. ISO/IEC 27001, IDW PS 951, VdS 10000).

☐ Im Unternehmen liegt eine Zertifizierung im Bereich des Datenschutzes vor.

2. Auftragskontrolle

Die Verarbeitung personenbezogener Daten im Auftrag darf nur nach Anweisung des Auftraggebers erfolgen

☒ Die Auswahl von externen Dienstleistern erfolgt unter Anwendung größter Sorgfalt (insbesondere bezüglich des Datenschutzes und der Informationssicherheit).

☒ Mit externen Dienstleistern, die personenbezogene Daten verarbeiten oder im Rahmen der Tätigkeit einsehen könnten, bestehen vertragliche Regelungen unter Einhaltung der Vorgaben aus Art. 28 der Datenschutzgrund-Verordnung bzw. EU-Standardvertragsklauseln.

☒ Die vereinbarten Kontrollrechte werden in regelmäßigem Abstand geltend gemacht (z.B. durch Einholung einer Bestätigung, eines Berichtes)

☒ Externe Dienstleister werden zur Verschwiegenheit verpflichtet.

☒ Daten bei externen Dienstleistern werden nach Auftragsende gelöscht.

Sonstige Maßnahmen:

ANHANG IV - LISTE DER UNTERAUFTRAGSVERARBEITER

ERLÄUTERUNG:

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

Die Dauer der Tätigkeit von Unterauftragnehmern (Laufzeit) für den Auftragsverarbeiter entspricht der Laufzeit der Rahmenvereinbarung mit dem Verantwortlichen.

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1	Name:	Horizon3 AI, Europe GmbH
	Anschrift:	Prielmayerstraße 3, D-80335 München, Amtsgericht Frankfurt am Main, HRB 127737
	Name, Funktion und Kontaktdaten der Kontaktperson:	Stefan Beck, Keyaccountmanager, stefan.beck@horizon3.ai
	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden) / Gegenstand und Art der Verarbeitung:	Autonomes Penetrationtesting
	Ort der Datenhaltung:	EU
2	Name:	Netcup
	Anschrift:	netcup GmbH Emmy-Noether-Straße 10 D-76131 Karlsruhe HRB 705547, Amtsgericht Mannheim
	Name, Funktion und Kontaktdaten der Kontaktperson:	Alexander Windbichler, Verantwortlicher nach § 18 MStV, alexander.windbichler@netcup.de
	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):	Hosting-Dienstleistungen

	Ort der Datenhaltung:	Deutschland
3	Name:	Telekom
	Anschrift:	Open Telekom Cloud / T-Systems International GmbH, Hahnstraße 43d, D-60528 Frankfurt am Main
	Name, Funktion und Kontaktdaten der Kontaktperson:	Datenschutzbeauftragten, Herrn Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.
	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):	Hosting-Dienstleistungen
	Ort der Datenhaltung:	Deutschland
4	Name:	Decareto
	Anschrift:	
	Name, Funktion und Kontaktdaten der Kontaktperson:	
	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):	Websitescans
	Ort der Datenhaltung:	Deutschland
5	Name:	Identeco
	Anschrift:	Identeco GmbH & Co. KG Joachimstraße 8 53113 Bonn
	Name, Funktion und Kontaktdaten der Kontaktperson:	Dr. Matthias Wübbeling, Geschäftsführer, matthias@identeco.de

	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):	Darknetscans
	Ort der Datenhaltung:	Deutschland
6	Name:	decareto GmbH
	Anschrift:	Mittelweg 144 20148 Hamburg
	Name, Funktion und Kontaktdaten der Kontaktperson:	Managing director: Eckhard Schneider, datenschutz@decareto.de
	Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden):	Webseitenscans
	Ort der Datenhaltung:	Deutschland

UNTERSCHRIFTEN

Diese Vereinbarung ist ohne Unterschrift gültig. Der Abschluss dieser Vereinbarung zur Auftragsverarbeitung erfolgt über die vertraglichen Regelungen in der Rahmenvereinbarung.