EUROPÄISCHE
KOMMISSION

Brüssel, den 4.6.2021
C(2021) 3701 final

ANNEX

ANHANG

des

Durchführungsbeschlusses der Kommission

über 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

[Geschäftlich]

STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von [zutreffende Option auswählen: **OPTION 1: 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]** oder [OPTION 2: Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG] 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.

[Geschäftlich]

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.

[Geschäftlich]

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

[Geschäftlich]

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

[Geschäftlich]

a) OPTION 2: ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: 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 **3 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 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.

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

[Geschäftlich]

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.

[Geschäftlich]

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.

[Geschäftlich]

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.

[Geschäftlich]

ANHANG I – LISTE DER PARTEIEN

Verantwortliche(r): [*Name und Kontaktdaten des/der Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten des Verantwortlichen*]

1. Name: Werbekunde (Werbekunde, der die AGB der Seeding Alliance GmbH akzeptiert hat.)

Anschrift:

Name, Funktion und Kontaktdaten der Kontaktperson:

Unterschrift und Beitrittsdatum: …

2.

…

Auftragsverarbeiter: [*Name und Kontaktdaten des/der Auftragsverarbeiter/s und gegebenenfalls des Datenschutzbeauftragten des Auftragsverarbeiters*]

1. Name: … Seeding-Alliance GmbH

Anschrift: … Ströer Allee 1; 50999 Köln

Name, Funktion und Kontaktdaten der Kontaktperson: Manager Data & Privacy; datenschutz@seeding-alliance.com

Unterschrift und Beitrittsdatum: Michael Dunker

…

2.

…

[Geschäftlich]

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

User

Kategorien personenbezogener Daten, die verarbeitet werden

Nutzungsdaten: URL; User-Agent, IP-Adresse)

Event-/Interaktionsdaten: Pageview; Hinzufügen eines Produkts zum Warenkorb oder Ansicht eines Produkts (auf Anfrage des Werbekunden)

Transaktionsdaten: (z. B. Kaufabgeschlossen, Produktmenge, Preis)

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 zutreffend

Art der Verarbeitung

Erheben, Weiterleiten, Löschen

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

Erfassung und Analyse von Nutzerinteraktionen mit Marketingmaßnahmen umfasst, um zu bestimmen, welche Aktionen zu Conversions führen und wie effektiv diese Maßnahmen sind.

Dauer der Verarbeitung

Max . 90 Tage

……

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

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

ERLÄUTERUNG:

Die technischen und organisatorischen Maßnahmen müssen konkret beschrieben werden; eine allgemeine Beschreibung ist nicht ausreichend.(siehe Anhang V)

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen)

zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

Maßnahmen zum Schutz der Daten während der Übermittlung

Maßnahmen zum Schutz der Daten während der Speicherung

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

Maßnahmen zur Gewährleistung der Datenminimierung

Maßnahmen zur Gewährleistung der Datenqualität

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss.

[Geschäftlich]

Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss

[Geschäftlich]

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).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1. Name: …Google Cloud (Rechenzentrum)

Anschrift: … 70 Sir John Rogerson's Quay; Dublin 2; Irland

Name, Funktion und Kontaktdaten der Kontaktperson: …

Beschreibung der Verarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden): …

Physische Speicherung der Daten

2. …

[Geschäftlich]

ANHANG V

Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DSGVO

Stand 25/10/2022, Version 1.2

[Geschäftlich]

I Vertraulichkeit (im Sinne von Art. 32 Abs.1 lit b DSGVO)

1. Maßnahmen zur Zutrittskontrolle

1.1 Maßnahmen zu Sicherheit der Rechenzentren

- Smart fencing
- Anticlimb fence;
- Fahrzeugschranken und laserbasierte Intrusion;
- Detection-Systeme, Biometrische;
- Identifikation, Metalldetektoren;
- Rundumüberwachung;
- Videoüberwachung (thermal Kameras und Standardkameras);
- Überwachung durch das Wachpersonal (24/7);
- Sicherheitsschlösser;
- Chipkarten-/Transponder-Schließsystem;
- Türsicherung (elektrischer Türschließer,
- Ausweisleser, Fernsehmonitor, Pförtner-24/7);
- Alarmanlage/Einbruchmeldesystem-24/7);
- Festlegung befugter Personen

(Betriebsangehörige und Betriebsfremde);

- Anwesenheitsaufzeichnungen;
- Besucherausweise zur Identifikation der Besucher;
- Protokollierung der Besucher (Besucherbuch)

1.2 Maßnahmen zur Sicherheit , vor unbefugtem Zutritt der Geschäftsstellen (Räume/Büros)

- Zutritt nur mit Schlüsselkarten;
- Einsatz von Wachpersonal;
- Sicherheitsschlösser;
- Chipkarten-/Transponder-Schließsystem
- Protokollierung der Besucher (Besucherbuch);
- Besucherausweise zur Identifikation und Firmenfremden;
- Schließung Fenster und Türen bei Abwesenheit / außerhalb der Arbeitszeit;
- Türsicherung (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner) Alarmanlage/Einbruchmeldesystem;

[Geschäftlich]

- Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz;
- Fremdfirmen unter Aufsicht
- Lichtschranken / Bewegungsmelder wenige Zugangswege; Gesicherter Eingang für An- und Ablieferung

1.3 Schutzmaßnahmen der Hardwarekomponenten vor Missbrauch

- Sicherheitsschlüssel für Client-Geräte und Server, Zwei-Faktor-Authentifizierung für Zugriff auf personenbezogene Daten.
- Zugriff auf Daten nur aus zugelassenen Netzwerken und Geo-Locations erlaubt.

1.4 Prüfung der umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit. Regelmäßige Prüfungen und Tests im Rechenzentrum

2. Maßnahmen zur Zugangskontrolle

2.1 Benutzerverwaltung

2.1.1 Vergabeverfahren von Benutzerzugängen

- Benutzerzugänge werden ausschließlich durch autorisiertes IT-Personal vergeben, wenn die Genehmigung der Geschäftsführung vorliegt.
- Benutzer, die personenbezogene Daten verarbeiten, erhalten den Zwang zur Zwei-Faktor-Authentifizierung mittels Smartphone.

2.1.2. Überprüfung der Gültigkeit von Benutzerzugängen

- Die Zugänge und dazugehörigen Rechte werden regelmäßig anhand der Aufgabenstellung des Mitarbeiters geprüft. Hierbei gilt immer das Minimalprinzip – ein Mitarbeiter erhält maximal die Rechte, die er für seine Tätigkeit zwingend benötigt. Benutzerzugänge werden nach Austritt eines Mitarbeiters sofort gesperrt.

2.1.3 Dokumentation der Benutzerzugänge

- Benutzerzugänge müssen formal beantragt werden. Dies geschieht durch den Benutzer selbst, oder einen autorisierten IT-Mitarbeiter i.A. für den Benutzer. Der Antrag enthält die erforderlichen Rechte in den Systemen. Die Geschäftsführung muss den Antrag genehmigen. Änderungen werden schriftlich festgehalten und müssen ebenfalls durch die Geschäftsführung genehmigt werden. Alle Genehmigungs- und Änderungsanträge werden nachvollziehbar protokolliert und archiviert.

2.1.4 Beschränkte Vergabe von Administrationszugängen

Administrativen Zugriff zu Systemen (z.B. Server) erhalten ausschließlich IT-Mitarbeiter, die über die aktuellen Sicherheitsbestimmungen im Unternehmen informiert und zur Umsetzung von Sicherheitsmechanismen angehalten werden. Nicht geschulte IT-Mitarbeiter, oder diejenigen, die keinen administrativen Zugriff auf Grund ihrer Tätigkeit benötigen, erhalten keinen administrativen Zugriff.

2.1.5 Voraussetzungen zu den Administratoren (fachlich und persönlich)

- Administratoren für IT-Systeme werden in verschiedenen Bereichen geschult (Datenschutz, IT- Sicherheit, Sicherung, operative Sicherheits- und-Zugriffsmechanismen)

2.1.6 Voraussetzungen zu den externen Administratoren, Service oder Wartungstechniker

• Externe/Dritte erhalten niemals administrativen Zugriff auf die personenbezogene Daten.

2.2 Passwortsicherheit

2.2.1 Sichere Speicherung der Passwörter, Verbot der Weitergabe an Dritte

• Passwörter werden verschlüsselt gespeichert und ausschließlich via sichere Verbindungen übertragen (SSL).

• Mitarbeiter sind zur Geheimhaltung ihrer Passwörter angehalten, die Weitergabe ist explizit verboten.

2.2.2 Anforderungen an die Komplexität von Passwörtern• Passwörter müssen bestimmte (Sonder-) Zeichen und Ziffern enthalten. Die Länge und Komplexität wird durch die Tätigkeit und Tiefe der Systemzugriffe (z.B. Administratoren) definiert.

• Je sensibler die Daten, je komplexer sind die Passwortrichtlinien. Die Passwortrichtlinien setzen sich aus 3 Stufen zusammen:

• Niedrig: Mindestens (jeweils) 8 Zeichen Gesamtlänge, darunter einen Buchstaben und eine Ziffer. Ein Buchstabe im Passwort muss großgeschrieben sein. Eine gleichartige Sequenz von Zeichen ist nicht erlaubt.

• Mittel: Mindestens (jeweils) 12 Zeichen Gesamtlänge, darunter einen Buchstaben, eine Ziffer und ein Sonderzeichen. Ein Buchstabe muss großgeschrieben sein. Eine gleichartige Sequenz von Zeichen ist nicht erlaubt.

• Hoch: Mindestens (jeweils) 32 Zeichen Gesamtlänge, einen klein- und einen großgeschriebenen Buchstaben, eine Ziffer und ein Sonderzeichen. Eine gleichartige Sequenz von Zeichen ist nicht erlaubt.

2.2.3 Gewährleistung der regelmäßigen Änderung von Passwörtern.

• Benutzer erhalten die Möglichkeit ihr Passwort zu ändern.

• Zusätzlich wird eine Zwei-Faktor-Authentifizierung eingesetzt, wodurch der Zwang nach Passwortwechsel entfällt.

2.2.4 Administration von Passwörtern

• Die Administration von Passwörtern und Erstvergabe von Passwörtern findet automatisiert anhand der unter I 2.2.2 genannten Passwortrichtlinien statt. Eine manuelle Vergabe von administrativen Mitarbeitern für andere Benutzer ist nicht möglich.

2.2.5 Abwehrmaßnahmen von unberechtigten Zugriffen bei gescheiterten Anmeldeversuchen Ein Benutzerzugang wird nach Fehlversuchen automatisch für eine bestimmte Zeit gesperrt. Länge und Anzahl der Fehlversuche richten sich nach der Sicherheitsstufe (definiert unter I 2.2.2).

• Niedrig: 5 Fehlversuche, Sperrung für 15 Minuten

• Mittel: 3 Fehlversuche, Sperrung für 30 Minuten

• Hoch: 3 Fehlversuche, Sperrung bis zur Aufhebung durch einen administrativen Benutzer. Automatische Mitteilung an IT-Security.

2.2.6 Organisatorischen Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz Regelmäßige Schulungen zum Umgang mit dem Arbeitsplatz-Geräten und Einweisungen zur Verhinderung von unberechtigten Zugriffen.

2.2.7 Weitere Maßnahmen zur Zugangskontrolle

- Einsatz von Verschlüsselungsroutinen für Dateien und Datenträgern (Geschäftsstelle Lüneburg);
- Zugang zu kabellosem Netzwerk verschlüsselt (WLAN);
- Kontrollierte Vernichtung von Datenträgern;
- Durchführung von Penetrationstests;
- Prozess bei Eintritt eines Mitarbeiters;
- Prozess bei Austritt eines Mitarbeiters;
- Richtlinien für die Dateiorganisation (Anlage in Projektordnern/Shares/etc.);
- Automatische Sperre Bildschirm/Arbeitsplatz bei Abwesenheit;
- Vergabe und Sicherung von Identifizierungsschlüsseln;
- Verpflichtung auf die Vertraulichkeit;
- Einsatz von Benutzernamen / Passwörtern für Daten und Programme;
- Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffssperren);
- Verschließbarkeit von Datenstationen;
- Einsatz einer aktuellen Firewall;
- Einsatz eines aktuellen Virenschutzes;
- Identifizierung eines Endgerätes/Terminals am IT-System

3 Maßnahme zur Zugriffskontrolle

3.1 Kontrolle zur Vergabe der Rollen/Zugriffsberechtigungen

- Benutzer erhalten im Zuge Ihrer Anlage in den Systemen eine Benutzer- und Sicherheitsrolle (siehe I 2.1.3 und I2.2.2).
- Die Vergabe von Rechten findet durch das 4-Augen-Prinzip statt (Administrative IT-Mitarbeiter und mindestens ein Mitglied der Geschäftsführung.

3.2 Dokumentation der Zugriffsberechtigungen

- Das Berechtigungskonzept wird durch Minimalismus und Zweck definiert. Benutzer erhalten maximal die Berechtigungen, die für ihre Tätigkeit erforderlich und den Zweck der Datenverarbeitung sinnhaft sind.

3.3 Kontrolle zur missbräuchlichen Verwendung der Zugriffsberechtigungen

- Der Zugriff und die Verarbeitung von personenbezogenen Daten werden protokolliert und mit einem Zeitstempel einem Benutzer zugewiesen.
- Durch Versionierung sämtlicher Datensätze sind Änderungen nachvollziehbar einem Benutzer und Zeitpunkt zuzuordnen. Zugriffe auf Datensätze werden ebenfalls protokolliert.

3.4 Weitere Maßnahmen zur Zugriffskontrolle

- Verwaltung der Benutzerrechte durch Systemadministratoren;

[Geschäftlich]

- Einsatz einer aktuellen Firewall;
- Einsatz einer zertifikatsbasierten Zugriffsberechtigung;
- Einsatz eines aktuellen Virenschutzes;
- Anzahl der Administratoren auf das Notwendigste reduziert;
- Einsatz eines zusätzlichen Accounts ohne Administratorberechtigungen bei Administratoren;
- Beschränkung der freien Abfragemöglichkeiten von Datenbanken (Query-Sprache)
- Benutzerbezogene Protokollierung der (Fehl-)Zugriffe;
- Einsatz von Aktenvernichtern; Einsatz von
- Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat) inkl. Protokollierung der Vernichtung;
- Datenschutzkonforme Löschung / Überschreibung vor Wiederverwendung von Datenträger;
- Einsatz von personifizierten Administratoraccounts;
- Einsatz von Verschlüsselungsroutinen für Dateien und Datenträgern;
- Protokollierung der Vernichtung von Daten;
- Prozess bei Eintritt eines Mitarbeiters;
- Prozess bei Austritt eines Mitarbeiters
- Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen entsprechend der Aufgaben der Mitarbeiter;
- Auswertung von Protokollen hinsichtlich Dateizugriff, IT-Systemnutzung, Firewalls, etc.;
- Management Logfiles: welche Berechtigungen wurden welchem Benutzer vergeben

4. Maßnahmen zur Trennbarkeit

4.1 Betroffene Maßnahmen um das Trennungsgebot, insbesondere in Bezug auf die Zweckgebundenheit der personenbezogenen Daten, zu gewährleisten

- Daten werden ausschließlich auf verschlüsselten Datenträgern und nach dem Zweck isolierten Systemen gespeichert.
- Nutzung von kundenspezifischen und mandantenfähigen Systemen

II Pseudonymisierung (bzw. Anonymisierung,) Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO). Die Seeding Alliance GmbH verfügt über Technologien, die die Ausspielung von Werbung in Form von Native Advertising ermöglichen. Dies stellt das Kerngeschäft der Seeding Alliance dar. Detaillierte Informationen zum Geschäftsmodell der Seeding Alliance GmbH finden Sie unter Punkt 5.1 der Datenschutzhinweise auf folgender Webseite: https://seeding-alliance.de/datenschutz/ . Dabei werden Scripte im Browser des Endnutzers (der betroffenen Person) geladen und ausgeführt. Durch diese Scripte weist die Seeding Alliance jedem Endnutzer eine User-ID (ein Pseudonym) zu.

Folgende mit der User ID verbundene Daten werden erhoben:

- Gerätebezogene Informationen

(gerätespezifische Informationen, z.B. das Modell der verwendeten Hardware, die Version des Betriebssystems, eindeutige Gerätekennungen, Informationen über das Mobilfunknetz des Endnutzers und Daten zu Geräteeigenschaften wie Browser-Typ, Browser-Sprache, Datum und Uhrzeit der Anfrage und Referrer-URL)

- IP Adressen. IP-Adressen der Betroffenen werden so geändert, dass ein Rückschluss auf die Nutzeridentität nicht mehr möglich ist (Anonymisierung). Anonymisierung erfolgt durch Kürzen von IP-Adressen (englisch: „truncating“) durch Entfernen des letzten Oktetts einer IP-Adresse;

III Integrität nach Artikel 32 Abs 1 lit b DSGVO

1. Maßnahmen zur Übertragungskontrolle

1.1 Integrität und Vertraulichkeit bei der Übertragung von personenbezogenen Daten Die Übertragung von Daten findet ausschließlich verschlüsselt und in der Regel durch vertragliche Bestimmungen abgesichert, statt

1.2 Verschlüsselungssystem bei der Übertragung von personenbezogenen Daten Für die verschlüsselte Übertragung von Daten an Dritte wird SSL (z.B. API-Zugriff) und SSH (z.B. Datenübertragung zw. Servern) eingesetzt.

1.3 Dokumentierung der Übertragung Datenübertragungen werden durch definierte Prozesse protokolliert (systemseitig) oder anhand von Empfängerlisten (E-Mail-Verteiler) gewährleistet.

1.4 Beschränkung des unberechtigten Abflusses von Daten Das Auslesen von Daten ist durch Benutzerrollen und technischen Zugriffsbestimmungen eingeschränkt und nur autorisiertem Personal erlaubt.

1.5 Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdeckt. Eine Aufdeckung eines unberechtigten Abflusses von Daten ist lediglich manuell möglich. Durch verschiedenste Sicherheitskonzepte wird die Gefahr eines unberechtigten Zugriffs jedoch massiv gesenkt. Siehe I 2.1.3, 2.2.2 und I 3.2 für weitere Informationen.

1.6. Weitere Maßnahmen zur Übertragungskontrolle

- Einsatz einer aktuellen Firewall;
- Einsatz eines aktuellen Virenschutzes;
- Einsatz von VPNs;
- Datenschutzkonforme Löschung;
- Überschreibung vor Wiederverwendung von Datenträger;
- Einsatz von Aktenvernichtern;
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung inkl. Protokollierung der Vernichtung;
- Einsatz von Verschlüsselungsroutinen für Dateien und Datenträgern;
- Festmontierte Plattenspeicher;
- Feststellung befugter Personen
- Gegenseitige Überwachung (4-Augen-Prinzip);
- Gesicherter Eingang Rechenzentrum für An- und Ablieferung

2 Maßnahmen zur Eingabekontrolle

2.1 Protokollierung und weitere Maßnahmen zur Eingabekontrolle

- Zugriffe von Benutzern werden für 90 Tage zum Zweck der Sicherheit und Erkennung von unzulässigen Zugriffen und Veränderungen von Daten gespeichert;
- Für wichtige und personenbezogene Daten wird eine Versionierung und ein Changelog eingesetzt, dass die Identifizierung von Eingaben/Ausgaben ermöglicht
- Einsatz elektronischer Signaturen

IV Verfügbarkeit und Belastbarkeit nach Artikel 32 Abs 1 lit b DSGVO

1.1 Organisatorische und technische Maßnahmen um im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten Für sämtliche Daten bestehen Backup- und Disaster-Recovery-Pläne. Daten werden in getrennten/verteilten Data-Center-Locations gespeichert und sind durch eine unabhängige Stromversorgung gesichert.

1.2 Schutzmaßnahmen von der elementaren Einflüssen (Feuer, Wasser usw.) Einsatz von Rauch- und Brandmeldern¬, Sprinkleranlagen; Brandschutztüren; Wasserschutzeinrichtungen.

1.3 Schutzmaßnahmen zur Bekämpfung von Schadprogrammen

- Firewalls, IDS-/IPS-Systeme;
- automatische Security-Patches auf die neuesten Versionen;
- Die Aktualität wird durch regelmäßige Updates der eingesetzt;
- Sicherheitslösungen eingehalten.

1.4 Maßnahmen zur rechtmäßigen Entsorgung der Dateiträger Datenträger werden durch das 4-Augen-Prinzip von 2 autorisierten Mitarbeitern des Rechenzentrums mit Protokollierung der Seriennummer des Datenträgers durchgeführt, bevor sie das Gelände des Rechenzentrums verlassen. Sollten Daten durch einen Hardwaredefekt der Datenträger nicht löschbar sein, werden sie sicher aufbewahrt bis eine physische Zerstörung des Datenträgers möglich ist.

IV Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen zur Sicherstellung der schnellen Wiederstellbarkeit Prüfung der Verfügbarkeit von erforderlichen Systemen, Datenträgern, Lizenzkeys, etc. zur Sicherstellung der schnellen Wiederherstellbarkeit von Daten und Programmen (Desaster-Recovery-Szenarien-siehe IV 1.1)

V Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung nach Artikel 32 Abs.1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)

1 Datenschutz-Management

1.1 Datenschutzorganisation

- DSB ist von außen bestellt;
- Ein Mitarbeiter ist als Datenschutzkoordinator tätig.

1.2 Maßnahmen zur Kontrolle der rechtmäßigen Verarbeitung der personenbezogenen Daten durch eigenen Mitarbeiter (bspw.; dass die Verarbeitung gemäß der Weisung des

[Geschäftlich]

Auftraggebers erfolgt)• Mitarbeiter werden durch Anweisungen und Schulungen darauf hingewiesen, welche Richtlinien einzuhalten sind.

- Jeder Mitarbeiter unterschreibt eine Geheimhaltungserklärung.

1.3 Gesetzeskonforme Verarbeitung durch die Mitarbeiter Verpflichtung der Mitarbeiter auf das Datengeheimnis, die Schulungen und Konzernrichtlinien

1.4 Kontrolle der Unterauftragsnehmer Unterauftragnehmer werden sorgfältig ausgewählt und erhalten ausschließlich Daten, die durch vertragliche Vereinbarungen zur Geheimhaltung und Einhaltung aller Datenschutzrichtlinien definiert sind.

1.5 Löschung/Venichtungsprozesse Daten die ihren Aufbewahrungszweck erfüllt haben, werden durch automatische Löschprozesse vernichtet. Sicherungsbedingte Kopien (z.B. Backups) werden zu diesem Zeitpunkt ebenfalls gelöscht.

1.6 Prüfung der internen Prozesse bzw. Arbeitsabläufe gemäß den jeweils aktuell gültigen Datenschutzbestimmungen. Regelmäßige Prüfung der aktuellen Abläufe und Schulung von Mitarbeitern

1.7 Sensibilisierung der Mitarbeitern in Bezug auf die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Durch IT Security und DS Richtlinien und regelmäßige Schulungen der Mitarbeiter wird sichergestellt, dass die Datenschutzbestimmungen und Richtlinien des Unternehmens eingehalten werden.

1.8 Datenschutzrechtliche Dokumentation Verfahrensverzeichnis; Verarbeitungsübersicht; Schwellwertanalyse; DSFA

2 Incident-Responce Management

- Die Mitarbeiter sind zum Verhalten bei Eintreten eines Datenschutzvorfalls sensibilisiert, ein Konzept bezüglich des Umgangs mit Datenpannen ist vorhanden;
- Gewährleistung von Reaktion und Kommunikation bei Datenschutzvorfällen;
- Gewährleistung von Meldepflichten und Fristen gegenüber Behörden bei Datenpannen

3 Datenschutzfreundliche Voreinstellungen

- Implementierung von datenschutzfreundlichen Voreinstellungen in Produkten;
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind (Zweckbindung, Datenminimierung);
- Zugriffsbeschränkung
- Anonymisierung
- Verschlüsselung
- Nutzerauthentifizierung
- Datensparsamkeit

VI Auftragskontrolle

Betroffene Maßnahmen zur Auftragskontrolle

- Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO;

- Weisungsbefugnisse sind festgelegt;
- Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation;
- Kontrolle der Vertragsausführung inkl. wirksamer Kontrollrechte;
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere bzgl. Datenschutz und Datensicherheit);
- Bestellung eines Datenschutzbeauftragten seitens des Auftragsverarbeiter;
- Sicherstellung der Rückgabe und/oder Vernichtung von Daten nach Beendigung des Auftrags;
- Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit Vertragsstrafen bei Verstößen