DataGuard

VERTRAG ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM SINNE DES ART. 28 ABS. 3 DER VERORDNUNG (EU) 2016/679 (DSGVO)

[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 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

Hinweis: dieses Dokument wurde auf der Grundlage des unter https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_part1_v5_0.pdf verfügbaren Textes der Europäischen Kommission erstellt.

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

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 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 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 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 [OPTION 1: Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 oder 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 zu unterstützen.

ABSCHNITT III – SCHLUSSBESTIMMUNGEN

Klausel 10

Verstöße gegen die Klauseln und Beendigung des Vertrags

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

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

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer

angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 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.

Hinweis: dieses Dokument wurde auf der Grundlage des unter https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_part1_v5_0.pdf verfügbaren Textes der Europäischen Kommission erstellt.

ANHANG I – LISTE DER PARTEIEN

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

1. Name: …
Anschrift: …
Name, Funktion und Kontaktdaten der Kontaktperson: …

Unterschrift und Beitrittsdatum: …

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

1. METAVITAL GmbH
Tannenhof 47, 22397 Hamburg
Name, Funktion und Kontaktdaten der Kontaktperson: Dr. Klaus Everding, Tannenhof 47, 22397 Hamburg

Unterschrift und Beitrittsdatum: 18.01.2023… Klaus Everding

Datenschutzbeauftragter des Auftragsverarbeiters:

DataCo GmbH

Dachauer Straße 65

80335 München

+49 89 7400 45840

www.dataguard.de

Hinweis: dieses Dokument wurde auf der Grundlage des unter https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_part1_v5_0.pdf verfügbaren Textes der Europäischen Kommission erstellt.

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden: Kunden.

Kategorien personenbezogener Daten, die verarbeitet werden: Gesundheitsdaten gem. Art. 4 Nr. 15 DS-GVO.

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: siehe Anlage TOM.

Art der Verarbeitung

- Fernzugriff
- Organisieren/Ordnen
- Speichern
- Auslesen
- Abfragen
- Löschen

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden: Support, Wiederherstellen der Funktionsfähigkeit des Systems, Upgrade der Software.

Die Dauer der Verarbeitung richtet sich nach den Bestimmungen des Reparaturauftrags, der als Leistungsvereinbarung zwischen den Parteien abgeschlossen wird.

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

Hinweis: dieses Dokument wurde auf der Grundlage des unter https://ec.europa.eu/info/sites/default/files/1_en_annexe_acte_autonome_part1_v5_0.pdf verfügbaren Textes der Europäischen Kommission erstellt.

ANHANG III

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN,

EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

METAVITAL GmbH

Datum: 22.06.2022

Generelle Informationen zum technischen Ablauf der Fernwartung/der Durchführung von Reparaturen vor Ort durch METAVITAL GmbH:

1. Fernwartung

In bestimmten Ausnahmefällen kann ein Zugriff auf die Systeme von METAVITAL GmbH zwecks Repara-tur erforderlich sein. Typische Konstellationen, bei denen sich eine Ferndiagnose bzw. Fernwartung an-bietet, sind:

- Überprüfungen, ob ein vom Kunden gemeldetes Problem auf einen Bedienungsfehler, einen Soft-waredefekt oder einen Hardwarefehler zurückzuführen ist
- Hilfestellung bei der Installation von Updates / Upgrades
- Beseitigung von typischen Softwarebugs (korrumpierte Zugangsberechtigung für den Kunden, be-schädigte Datenbank, beschädigte Konfigurationen oder Skripte).

In diesen Fällen können unsere Techniker Zugriff auf personenbezogene Daten, einschl. besonders sen-sib-lerDaten erhalten, welche sich auf dem Endgerät des Kunden befinden. In Einzelfällen kann dieser Zugriff auf Daten nicht vermieden werden.

Zur Durchführung von Fernwartung wird das Tool Teamviewer eingesetzt. Der Kunde muss der Fernwar-tung explizit zustimmen, indem er eine mehrstellige Kennziffer an die Techniker von METAVITAL GmbH übermittelt. Danach erhält der Techniker von METAVITAL GmbH Zugriff auf das Endgerät des Kunden. Die nachgelagerte Kommunikation mit dem Endgerät des Kunden wird mit 256-Bit verschlüsselt. Der Kunde kann jederzeit am heimischen Endgerät die Aktionen des Technikers von METAVITAL GmbH beobachten. Auf Seiten von METAVITAL GmbH werden sämtliche Aktionen, die im Rahmen der Sitzung per Teamvie-wer stattfinden, protokolliert und in einer Log-Datei erfasst. Nach erfolgter Fernwartung erhält sowohl der Kunde als auch METAVITAL GmbH die Dokumentation des Vorgangs in Form dieser Log-Datei.

2. Durchführung von Reparaturen vor Ort

Der Kunde hat zusätzlich die Möglichkeit, die Systeme von METAVITAL GmbH in den Unternehmens-räum-lichkeiten von METAVITAL GmbH durch unsere Techniker reparieren zu lassen. Zu diesem Zweck muss der

Kunde das System an METAVITAL GmbH senden. METAVITAL GmbH hat organisatorische Maß-nahmen getroffen, damit in diesen Fällen grundsätzlich. keine Verarbeitung personenbezogener Daten einschl. besonders sensibler Daten des Kunden durch METAVITAL GmbH stattfindet. Im Reparaturauftrag werden die Kunden aufgefordert, die medizinische Datenbank und etwaige personenbezogene Daten zu sichern und von ihren Systemen zu löschen, bevor sie diese bei METAVITAL GmbH einsenden. Die Kun-den dokumentieren den Vorgang durch Ankreuzen einer Checkbox im Reparaturauftrag, der sodann als Bestätigung an METAVITAL GmbH zurückgesendet wird.

Sobald das Endgerät des Kunden bei METAVITAL GmbH eintrifft, kontrollieren unsere Techniker, ob die Löschung tatsächlich erfolgt ist. Zu diesem Zweck wird eine gezielte Suche nach entsprechenden Datei-namen in den vorgesehenen Ordern durchgeführt, ohne dass die Techniker von METAVITAL GmbH Kenntnis von dem Inhalt der Dateien erlangen. Falls - wider Erwarten - personenbezogene Daten auf der Endeinrichtung des Kunden vorhanden sind, wird der Kunde kontaktiert und über diesen Umstand in-formiert. Dem Kunden wird sodann seitens METAVITAL GmbH angeboten, die vorhandenen personen-bezogenen Daten auf einem externen Datenträger zu sichern, um die Verfügbarkeit der Daten zu ge-währleisten. Dabei wird sichergestellt, dass der Kunde die alleinige Entscheidungsbefugnis über die ge-speicherten personenbezogenen Daten behält. Wenn er mit dem Vorschlag von METAVITAL GmbH nicht einverstanden ist, kann er die Sicherung auf dem externen Datenträger verweigern und diese selbst vor-nehmen. Zu diesem Zweck würde METAVITAL GmbH das Endgerät an den Kunden zurücksenden.

Falls der Kunde sein Einverständnis mit dem Vorschlag von METAVITAL GmbH äußert, werden personenbezogene Daten auf einem externen Datenträger gesichert und vom Endgerät des Kunden gelöscht. Nach Durchführung der Reparatur/Wartung werden die Daten wieder auf das System aufgespielt und anschließend von dem externen Datenträger vollständig gelöscht. Der Kunde wird in jedem Fall aufge-fordert, in Zukunft der Aufforderung zum Löschen der personenbezogenen Daten einschl. besonders sensiblen Daten nachzukommen.

Sofern nicht anders angegeben, handelt es sich bei den nachstehend genannten TOM um Maßnahmen, die im Rahmen der Fernwartung und/oder des durchzuführenden Reparaturauftrags durch METAVIAL GmbH implementiert wurden.

Zutrittskontrolle

☒ Physische Absicherung der Unternehmensräumlichkeiten

Abschließbare Türen, Sicherheitsschlösser

☒ Zusätzliche Absicherung der Räumlichkeiten

Videoüberwachung, Alarmanlage nach Dienstschluss

☒ Schlüsselregelung

Die Beschäftigten erhalten Zugang mit Schlüssel für ihren Arbeitsbereich

☒ Zutrittsorganisation

Zutrittsberechtigt sind ausschließlich die Beschäftigten von METAVITAL GmbH. Fremdpersonen (wie z.B. Kunden, Paketlieferdienste) dürfen die Räumlichkeiten von METAVITAL GmbH ausschließ-lich unter Aufsicht, die während der ganzen Anwesenheit andauert, betreten

☒ Beschränkung der Zutrittsberechtigungsstruktur auf das Notwendigste

Diese Beschränkung der Zutrittsberechtigungsstruktur gilt auch für den Zutritt zum Server

☒ Zusätzliche Absicherung des Servers

Der Serverschrank ist stets abgeschlossen, außer wenn physischer Zugriff in eng begrenzten Fällen erforderlich ist

☒ Sonstige ergriffene Maßnahmen im Hinblick auf die Fernwartung

Die Arbeit mit Kundensystemen (sowohl die Fernwartung als auch die Reparatur vor Ort) darf aus-schließlich von den qualifizierten Technikern von METAVITAL GmbH und in den unternehmensinternen Techniker-räumen von METAVITAL GmbH vorgenommen werden

Datenträgerkontrolle

☒ Verzeichnis von Datenträgern

Es wird ein internes Verzeichnis der Datenträger von METAVITAL GmbH geführt.

Zusätzlich wird ein Verzeichnis von Datenträgern geführt, die von Kunden angeliefert werden (die Listung und Dokumentation erfolgt in diesem Fall im Wareneingang). Dies wird dann vorgenom-men, wenn Wartungsarbeiten am System des Kunden durchzuführen sind, die einen physischen Zugriff auf das System des Kunden erfordern.

☒ Abgeschlossene Lagerung von Datenträgern nach Dienstschluss

Datenträger finden sich während der ganzen Reparatur am Arbeitsplatz der Techniker und werden nach Dienstschluss in einem abschließbaren Stahlschrank aufbewahrt.

Zugangskontrolle

Die nachstehenden Maßnahmen beziehen sich generell auf den Zugang zu den Rechnersystemen der Techniker von METAVITAL GmbH

☒ Authentifizierung von Benutzern

Authentifizierung mittels Benutzername & Passwort

☒ Passwortrichtlinie und systemseitige Forderung der Passwortanforderungen

☒ Passwortkomplexität

Mind. 3 der 4 Kriterien: Großbuchstabe, Kleinbuchstabe, Sonderzeichen und Zahl

☒ Es werden Passwörter mit einer Mindestlänge von 8 Zeichen verwendet

☒ Kein zeitbasierter Wechsel von Passwörtern (nur anlassbezogen)

☒ Sperrung des Systemzugangs nach definierter Anzahl von Falschanmeldungen

Eine Sperrung erfolgt nach 10 Fehlversuchen

☒ Gruppenweiter Auto-Logout nach definierter Zeit

Nach 30 Minuten Abwesenheit findet ein Auto-Logout an jedem Arbeitsplatz-PC

Benutzerkontrolle

☒ Verpflichtung der Beschäftigten von METAVITAL GmbH auf Vertraulichkeit

☒ Schriftliche Regelung zum Umgang mit elektronischen Betriebsgeräten

☒ Schriftliche Regelung zum Umgang mit personenbezogenen Daten (Clean Desk Policy)

☒ Need-to-know bzw. Principle of Least Privilege implementiert

Die Berechtigungsstruktur ist auf das Notwendigste beschränkt

☒ Regelmäßige Schulungen zum Thema Datenschutz

Die Datenschutz-Schulungen finden mindestens 1x/Jahr statt und werden durch METAVITAL GmbH dokumentiert.

☒ METAVITAL GMBH hat einen externen Datenschutzbeauftragten bestellt

Transportkontrolle

☒ Regelungen zur physischen Datenübermittlung

Bei Papierdokumenten: Versandbestätigungen und verschließbare Mappen. Beim Versand der Kundensysteme per Versanddienstleister werden die Pakete ausschließlich versichert übersandt.

Übertragungskontrolle und Datenintegrität

☒ VPN-Tunnel; Regelungen für Heim-/Auswärtstätigkeiten

☒ Firewall, Antivirensoftware

☒ Sonstige ergriffene Maßnahmen

Dem Kunden ist die Verbindung der Endeinrichtung mit dem Internet oder einem lokalen Netzwerk ausschließlich zum Einspielen von Updates oder nach ausdrücklicher Aufforderung durch den zu-ständigen Techniker von METAVITAL GmbH gestattet. Dabei handelt es sich um eine vertragliche Pflicht des Kunden, die in dem Vertrag mit METAVITAL GmbH festgelegt ist.

Wiederherstellbarkeit

☒ Datensicherungskonzept (Backup-Konzept)

Für die Sicherung personenbezogener Daten, die auf dem Endgerät gespeichert sind, ist primär der Kunde verantwortlich. Hierzu wird er auch explizit vor dem Einsenden des Endgeräts seitens ME-TAVITAL GmbH aufgefordert. Im Rahmen der angebotenen Dienstleistung (Fernwar-tung/Durchführung von Reparaturarbeiten) wird dem Kunden die Sicherung der gespeicherten personenbezogenen Daten angeboten, falls diese Daten – wider Erwarten – von dem Endgerät nicht gelöscht wurden. Alle Elemente der für den Betrieb des Systems notwendigen Software, die Updates, Upgrades und Patches können von METAVITAL jederzeit wieder hergestellt werden.

☒ Sichere Aufbewahrung der Datensicherungen

Die Datensicherungen werden auf externen Festplatten gespeichert und sicher aufbewahrt (s. Ab-schnitt ,,Datenträgerkontrolle“)

Zuverlässigkeit

☒ Datenschutz-Managementsystem

☒ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit

der technischen und organisatorischen Maßnahmen

Nachvollziehbarkeit

☒ Protokollierung von Zugriffen auf die Systeme des Kunden

Auf Seiten von METAVITAL GmbH werden sämtliche Aktionen, die im Rahmen der Sitzung per Teamviewer stattfinden, protokolliert und in einer Log-Datei erfasst. Nach erfolgter Fernwartung erhält sowohl der Kunde als auch METAVITAL GmbH ein Exemplar der Log-Datei. Auf diese Weise erhält der Kunde die erforderliche Dokumentation des Vorgangs.

☒ Protokollierung von Verarbeitungsvorgängen (Eingabe, Änderung und Löschung von

Daten)

s.o.

Hiermit akzeptiere ich die in dieser Auftragsverarbeitungs-Vereinbarung und in den drei Anhängen dargelegten Bestimmungen.

Ort, Datum | Unterschrift Auftraggeber*in

Ort, Datum | für **METAVITAL** GmbH, Unterschrift