Präambel zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 (3) Verordnung (EU) 2016/679 ("DSGVO") auf Basis der EU-Standardvertragsklauseln („Auftragsverarbeitungsvertrag“).

Diese Vereinbarung gilt zwischen dem jeweiligen Vertragspartner („Auftraggeber“), in dessen Funktion als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO[1] und der SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden, in ihrer Funktion als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO, nachstehend „Auftragnehmer“, „SVA“ oder „Auftragsverarbeiter“ genannt.

Mit Beauftragung der SVA durch den Auftraggeber aber spätestens durch den Abschluss einer datenschutzrechtlich relevanten Leistungsvereinbarung, schließen die Parteien diesen Auftragsverarbeitungsvertrag auf Basis der EU-Standardvertragsklauseln.

Um den Prüfungsaufwand für alle Beteiligten so gering wie möglich zu halten, gleichzeitig aber eine faire und transparente vertragliche Datenschutzregelung sicherzustellen, nutzen wir für unsere Vereinbarung zur Auftragsverarbeitung die Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern innerhalb EU/EWR gemäß Artikel 28 Absatz 7 DSGVO. Neben den Standardvertragsklauseln für den Drittlandtransfer hat die EU auch Standardvertragsklauseln zur Verwendung innerhalb der EU/EWR bereitgestellt. Dieser durch die EU-Kommission im Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021 veröffentlichte Standardvertrag schreibt grundsätzlich eine Unabänderbarkeit der Klauseln vor, welche aber durch eine Erweiterung (Klausel 11 und Anlagen) ergänzt werden kann, sofern diese nicht in einem Widerspruch zu den Regelungsinhalten der Standardvertragsklauseln stehen. Durch uns erfolgte keine Anpassung der vorgegebenen Klauseln. Die wie vorgesehen individuell durch uns angepassten Abschnitte sind in Klausel 11 und den entsprechenden Anlagen zu finden.

Anwendungsbereich
Dieser Auftragsverarbeitungsvertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den vereinbarten Leistungen ergeben. Dieser Vertrag erstreckt sich somit auf jegliche Tätigkeiten, die als Auftragsverarbeitungen i.S.d. Art. 28 DSGVO anzusehen sind. Dies kann gem. der Auslegung der nationalen Aufsichtsbehörden und des europäischen Datenschutzausschusses auch Tätigkeiten beinhalten, bei denen zwar eine Verarbeitung von personenbezogenen Daten nicht unmittelbar Gegenstand der beauftragten Leistung ist, ein Zugriff auf solche Daten jedoch bei der Leistungserbringung nicht ausgeschlossen werden kann (z.B. bei (Fern-)Wartung von IT-Systemen durch SVA).

Anwendbarkeit und Vorrangregelung
Dieser Vertrag kann jederzeit durch eine zwischen den Parteien verhandelte Individualvereinbarung ersetzt oder ergänzt bzw. konkretisiert werden – in solchen Fällen, können Sie sich an datenschutz@SVA.de wenden. Sofern zwischen den Vertragsparteien für den jeweiligen Verarbeitungsgegenstand bereits eine vertragliche Regelung zur Auftragsverarbeitung gem. Art 28 (3) DSGVO besteht, hat diese Anwendungsvorrang gegenüber diesem Vertrag.

Sollte aufgrund der Art, des Umfangs oder der Natur der Zusammenarbeit, der personenbezogenen Daten oder der Verarbeitungstätigkeit die Notwendigkeit bestehen, eine Individualvereinbarung abzuschließen, wird diese durch beide Parteien im Benehmen beschlossen. Dies gilt insbesondere, insofern dies aufgrund einer rechtlichen Anforderung oder unter Betrachtung der Risiken für die Rechte und Freiheiten der betroffenen Personen als erforderlich anzusehen ist. Der Bedarf an einer Individualvereinbarung kann zudem bei Einsatz eines zustimmungsbedürftigen Unterauftragsverarbeitungsverhältnisses bestehen.

[1] (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).

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

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) 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 zwei Wochen 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 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 oder 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 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.

Klausel 11
(Ergänzungen zu den Standardvertragsklauseln durch die Vertragsparteien)

11.1 Rechtswahl und Gerichtsstand

a) Dieser Vertrag und alle im Rahmen seiner Durchführung geschlossenen Rechtsgeschäfte unterliegen deutschem Recht und soweit anwendbar der DSGVO. Internationales UN-Kaufrecht (UNCITRAL) und die Verweisnormen des Internationalen Privatrechts sind ausgeschlossen.

b) Die Parteien vereinbaren für alle Rechtsstreitigkeiten, die sich aus oder in Zusammenhang mit diesem Vertrag ergeben, dass die zuständigen Gerichte die des Sitzes des Verantwortlichen bzw. Auftraggebers sind.

11.2 Verantwortlichkeiten und Rollen der Vertragsparteien

a) Alle in diesem Vertrag dargelegten Verweise auf den Verantwortlichen und dessen Rechte und Pflichten sind in Fällen, in denen beide Vertragsparteien als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO agieren, auf den beauftragenden Auftragsverarbeiter (Auftraggeber) anzuwenden, der den weiteren Auftragsverarbeiter (Auftragnehmer) in Anspruch nimmt.

b) Wird der Vertrag direkt zwischen einem Verantwortlichen (Auftraggeber) und einem Auftragsverarbeiter (Auftragnehmer) geschlossen, so gelten die in diesem Vertrag dargelegten Vereinbarungen dem Wortlaut entsprechend.

11.3 Regelung zu verbundenen Unternehmen

a) Die Vereinbarungen dieses Vertrages finden auch Anwendung für mit dem Auftraggeber (vgl. §§ 15 ff. AktG, § 271 Abs. 2 HGB) verbundene Unternehmen.

b) Die mit dem Auftraggeber verbundenen Unternehmen tragen die entsprechenden Rechte und Pflichten aus diesem Vertrag, wie die zum Vertragsschluss berechtigte Partei selbst.

c) Für verbundene Unternehmen nach diesem Vertrag haftet die zum Vertragsschluss berechtigte Partei ggü. dem Auftragsverarbeiter, wie für eigenes Verschulden, gemäß Klausel 10 dieses Vertrages.

d) Die Parteien können eine Liste von zur Beauftragung berechtigten verbundenen Unternehmen in einer Anlage zu dieser Vereinbarung konkretisieren. Soweit vorhanden, ist diese Anlage als „Anhang V“ zu diesem Vertrag anhänglich.

11.4 Kündigungsregelung

a) Die Kündigungsfrist dieses Vertrages entspricht der/des zugrundliegenden Servicevertrages bzw. Leistungsvereinbarung.

b) Das Kündigungsrecht nach Klausel 10 dieses Vertrages bleibt unberührt.

c) Wird dieser Vertrag gekündigt, ist die Fortführung einer Verarbeitung von personenbezogenen Daten ausgesetzt, bis der gekündigte Vertrag durch einen rechtswirksamen neuen Vertrag ersetzt ist.

11.5 Verarbeitung außerhalb von Geschäftsräumen

a) Soweit nicht anderweitig vereinbart, ist die Verarbeitung von Daten außerhalb der Räumlichkeiten des Auftragsverarbeiters zulässig. Ein aussagekräftiges Dokument über die Absicherung der Verarbeitung ist dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.

b) Der Auftragsverarbeiter stellt sicher und sichert zu, dass die Einhaltung von allen erforderlichen und adäquaten Maßnahmen zum Datenschutz im Sinne des Art. 32 DSGVO auch in Fällen des 11.5 (a) sichergestellt ist.

11.6 Einsatz von Zertifikaten als Nachweis einer ordnungsgemäßen Verarbeitung

Durch geeignete und gültige Zertifikate zur IT-Sicherheit und Datenschutz (z.B. IT-Grundschutz, ISO 27001, etc.) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht das Recht des Auftraggebers zur Überprüfung noch die Pflicht der Auftragnehmers zur Dokumentation der Sicherheitsmaßnahmen im Sinne der Klausel 7.6 dieses Vertrages.

11.7 Ergänzende Klausel zu 7.7 a) Einsatz von Unterauftragsverarbeitern

In Fällen des betrieblichen Notstands wie z.B. Serverausfällen und Cyberangriffen mit massiven Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs der/des Verantwortlichen oder die Sicherheit der personenbezogenen Daten der betroffenen Personen ist der Auftragsverarbeiter nach Unterrichtung des Auftraggebers berechtigt, weitere Unterauftragsverarbeiter für den begrenzten Zeitraum des Krisenfalls einzuschalten. Der in Klausel 7.7 a) dieses Vertrags definierte Unterrichtungszeitraum verkürzt sich hierdurch zugunsten einer kurzfristigen Bekanntgabe des einzusetzenden Unterauftragsverarbeiters vor Verarbeitungsbeginn. Das dem Auftraggeber in diesem Zusammenhang zustehende Widerspruchsrecht bleibt bestehen.

11.8 Geheimhaltung und Vertraulichkeit

a) Der Auftragsverarbeiter ist verpflichtet, seine Beschäftigten und Erfüllungsgehilfen, die an der Verarbeitung personenbezogener Daten oder anderer vertraulicher oder geheimhaltungsbedürftiger Informationen beteiligt sind, gemäß den entsprechenden rechtlichen Vorschriften (u. a. § 2 GeschGehG, § 3 TTDSG, § 53 BDSG, § 203 StGB) dokumentiert zu belehren und zu verpflichten. Belehrung und Verpflichtung bestehen auch nach Beendigung der Tätigkeit fort.

b) Der Auftragsverarbeiter sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragsverarbeiter sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet hat, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

11.9 Schriftform und Salvatorische Klausel

a) Änderungen und Ergänzungen dieses Vertrags und aller Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt, was auch in einem elektronischen Format erfolgen kann.

b) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Die Parteien werden diese Bestimmung dann durch eine Bestimmung ersetzen, die den angestrebten Regelunszweck der unwirksamen, bzw. nicht durchsetzbaren bzw. nicht durchführbaren Bestimmung – soweit rechtlich zulässig – erreicht bzw. am nächsten kommt. Das gilt insbesondere für Regelungslücken in diesem Vertrag.

11.10 Haftung

a) Jede Partei haftet gegenüber der anderen Partei für Schäden, die sie der anderen Partei durch einen schuldhaften Verstoß gegen geltende datenschutzrechtliche Bestimmungen verursacht, gem. den Regelungen der DSGVO.

b) Für Pflichtverletzungen aus dieser Vereinbarung zur Auftragsverarbeitung gilt entsprechend das in der DSGVO festgelegte Haftungsregime, das eine vertraglich unbeschränkte Haftung nach den gesetzlichen Bestimmungen vorsieht. Etwaige zwischen den Parteien vereinbarte Haftungsbeschränkungen aus anderen Verträgen sind auf datenschutzrechtliche Belange nicht anzuwenden und entfallen zugunsten der in diesem Vertrag getroffenen Regelung.

ANHANG I – LISTE DER PARTEIEN

1. Name und Anschrift Auftraggeber: Beauftragende Partei gem. Leistungsvereinbarung.

- Kontaktdaten des Datenschutzbeauftragten: Vom Auftraggeber bereitzustellen (z. B. über die Website oder per E-Mail-Benachrichtigung).
- Rolle: Auftraggeber
- (Beitritts-)Datum: Entspricht dem Datum der Beauftragung auf Basis der Leistungsvereinbarung.

2. Name und Anschrift Auftraggnehmer: SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden

- Kontaktdaten des Datenschutzteams und der/des Datenschutzbeauftragten der SVA:
  - Datenschutzteam: datenschutz@sva.de, +49 6122 536-0
  - Datenschutzbeauftragte(r): dsb@sva.de, +49 6122 536-0
- Rolle: Auftragnehmer (Auftragsverarbeiter)
- (Beitritts-)Datum: Entspricht dem Datum der Beauftragung auf Basis der Leistungsvereinbarung

ANHANG II – BESCHREIBUNG DER VERARBEITUNG

Für alle aufgezählten Kategorien betroffener Personen und personenbezogener Daten gilt: Der Auftraggeber hat dem Auftragnehmer von den hier genannten abweichende personenbezogene Daten mitzuteilen. Die in dieser Mitteilung aufgeführte Anpassung der personenbezogenen Daten wird als Ergänzung ein Bestandteil dieser Vereinbarung. Hierzu zählen auch personenbezogene Daten, zu denen der Auftraggeber dem Auftragnehmer in Verbindung mit der Bereitstellung von Produkten oder Diensten Zugang gewährt. Soweit nicht anders vereinbart, gelten die Bestimmungen dieses Vertrages zur Auftragsverarbeitung entsprechend.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Kategorien betroffener Personen, kann die Datenverarbeitung prinzipiell sämtliche Personenkategorien umfassen, die der Verantwortliche verarbeitet und im Kontext der vereinbarten Leistung im Zugriffsbereich des Auftragnehmers stehen könnten oder anderweitig verarbeitet werden müssen bzw. könnten. Dies kann beinhalten:
- beschäftigte Personen i.S.d. § 26 BDSG,
- Endkunden/Kunden,
- Lieferanten,
- Sonstige (z. B. Bürgen, andere Dritte wie Steuerberater etc.).

Kategorien personenbezogener Daten, die verarbeitet werden

Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Arten personenbezogener Daten kann die Datenverarbeitung prinzipiell sämtliche Kategorien und Arten umfassen, die der Verantwortliche verarbeitet und im Kontext der vereinbarten Leistung im Zugriffsbereich des Auftragnehmers stehen könnten oder anderweitig verarbeitet werden müssen bzw. könnten. Diese können umfassen:
- Allgemeine Personendaten (z. B. Vor- und Nachname, Adresse, etc.)
- Ordnungsdaten (z. B. Kunde-Nr., Mitarbeiter-Nr., Mitglieds-Nr. etc.)
- Vorgangsdaten IT-Servicemanagement (z. B. Endanwender-Kontaktdaten, Historie Daten, etc.)
- Logdaten (z. B. User-Historie, Änderungshistorie, Account-Nutzungsdaten etc.)
- Telekommunikationsdaten (§ 3 TTDSG)

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:

- besondere Arten von personenbezogenen Daten (Art. 9 DSGVO)

Art der Verarbeitung

Der Auftragnehmer führt im Auftrag des Auftraggebers (IT-)Dienstleistungen durch. Die Art der Verarbeitung ergibt sich aus den korrespondierenden Leistungsverträgen. Dies umfasst somit prinzipiell die beiläufige Einsichtnahme und die nicht auszuschließende Verarbeitung bei Erbringung von (IT-)Dienstleistungen, als auch eine geplante Verarbeitung auf Basis der Leistungsbeschreibung.

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

Support und (IT-)Dienstleistungen, exemplarisch im Rahmen von Inbetriebnahme, Installation und Wartung von Hard- und Software des Auftraggebers, Hosting-Services sowie sonstige Leistungen aus dem Portfolio des Auftragsverarbeiters.

Dauer der Verarbeitung und Vertragslaufzeit

Die Dauer der Verarbeitung und Laufzeit dieser Vereinbarung entspricht der Dauer der korrespondierenden, vereinbarten Leistung(en) gem. der zugehörigen Lesitungsvereinbarung.

ANHANG III – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Durch die SVA wurden die nachfolgend dokumentierten technischen und organisatorischen Schutzmaßnahmen getroffen.

Dieses geschieht unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Die SVA trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken berücksichtigt, die mit der Verarbeitung verbunden sind, z.B. durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

Sofern die zu erbringende Leistung des Auftragnehmers ausschließlich in den Räumlichkeiten des Verantwortlichen bzw. Auftraggebers, unter ausschließlichem Einsatz dessen technischer Systeme bzw. Datenverarbeitungsanlagen und unter der Weisung bzw. Aufsicht des Verantwortlichen bzw. Auftraggebers erfolgt, treten anstelle der in dieser Anlage hinterlegten technischen und organisatorischen Schutzmaßnahmen diejenigen des Verantwortlichen bzw. Auftraggebers.

Wird dieser Vertrag zwischen SVA und einem Auftragnehmer bzw. Unterauftragnehmer geschlossen, können diese alternative technische und organisatorischen Schutzmaßnahmen ergreifen, sofern die nachstehenden Schutzmaßnahmen nicht unterschritten werden. Diese sind zu dokumentieren und als Anhang zu dieser Vereinbarung anhänglich. Soweit ein solcher Anhang zu dieser Vereinbarung nicht ersichtlich ist, gelten die nachfolgenden technischen und organisatorischen Schutzmaßnahmen als vom Auftragnehmer bzw. Unterauftragnehmer erfüllt.

Pseudonymisierung

Grundsätzlich ist eine Pseudonymisierung im Rahmen der Leistungserbringung nur möglich, wenn die Verarbeitung oder Übermittlung der Daten auf Systemen erfolgt, die der Verantwortung der SVA unterliegen. Die SVA kann verschiedene Pseudonymisierungsmethoden einsetzen. Das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen wesentlich zu erschweren, erfolgt auf Weisung des Kunden.

1 Zutrittskontrolle

Maßnahmen, die verhindern, dass unbefugte Personen physischen Zutritt zu Datenverarbeitungsanlagen erhalten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Perimeterschutz abhängig vom Objekt und darin enthaltenden schützende Systeme	Empfang / Rezeption
Automatisches Zutrittskontrollsystem (personalisierte elektronische SVA-Schließkarten)	Besucherbuch / Protokollierung der Besucher
Chipkarten / Transpondersysteme	Mitarbeiter- / Besucherausweise
SVA Schließsystem	Begleitungspflicht für Besucher durch SVA-Mitarbeiter
24x7 Videoüberwachung im Rechenzentrum	Richtlinie Umgang mit Schlüsseln
Klingel- Türsprechanlagen	Schlüsselregelung und -liste
Protokollierung der Zutritte durch das SVA Schließkartensystem	Unterschiedliche Zutrittssicherheitszonen nach Schutzbedarf
Zugang zum Rechenzentrum erfolgt über 2 FA	Richtlinie zum Umgang mit Besuchern und Lieferanten
24x7 Videoüberwachung des Firmengeländes (Hauptstandort)	Individuelle Vergabe der Zutrittsrechte nur im erforderlichen Umfang

2 Zugangskontrolle

Verhinderung, dass die Nutzung der Datenverarbeitungsanlagen durch Unbefugte erfolgt.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit personalisierten Benutzeraccounts	Sichere Passwortvergabe
Multi-Faktor-Authentisierung (systemabhängig)	Richtlinie Umgang mit Zugängen und Passwörtern
Automatische Sperrung von Konten bei zu vielen gescheiterten Anmeldeversuchen	Richtlinie zum aufgeräumten Arbeitsplatz
Protokollierung der Systemanmeldungen	Richtlinie Umgang mit mobilen Geräten
Anti-Viren-Software Server/Clients	Richtlinie Löschen / Vernichten
Firewall	Aufgaben- /Funktionstrennung
Intrusion Detection Systeme (IDS)	Rollen- und Berechtigungskonzepte
Mobile Device Management für alle mobilen Endgeräte	Regeln und Verfahren zur Netzwerksegmentierung werden umgesetzt
VPN bei Remote-Zugriffen	Richtlinie „Arbeiten und Verhalten in Sicherheitsbereichen“
Bereitstellung eines Passwort-Managers	Richtlinie mobilen Arbeiten
Automatische Bildschirmsperre bei Inaktivität	Richtlinie Umgang mit Druckern
Patchmanagement	
Geschützter Druck	
Härtungsmaßnahmen werden für Betriebssysteme und Anwendungen umgesetzt	
Jährliche Überprüfung der Sicherheitsmaßnahmen durch Penetrationstest	
Zugangskontrolle für Clients auf Netzwerkebene	

3 Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugriffsberechtigung umfassten, personenbezogenen Daten Zugriff haben.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Manipulationssicherheit der Zugriffsprotokollierung	Beschränkung der User-Anzahl mit Administratorenrechten auf das notwendige Minimum
Separierung und Verwaltung privilegierter Zugänge	Verwaltung Benutzerrechte durch Administratoren
Sichere Löschung von Daten/-trägern	Rollen- und Berechtigungskonzept
Sichere Vernichtung nach DIN 66399	Genehmigungsverfahren für Rechtevergabe, -änderung, -entzug
Verschlüsselung Notebooks/Smartphones	Protokollierung von allen Rechteänderungen
Eine Segmentierung der genutzten Netze ist definiert	Umsetzung des „Need-to-Know“ Prinzips
Systemabhängige Zugriffsprotokollierung	

4 Trennungskontrolle

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Mandantentrennung	Aufgaben- /Funktionstrennung
Trennung von Produktions- und Testdaten	
Logische Trennung von Daten	

5 Weitergabekontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport die Vertraulichkeit und Integrität der Daten geschützt werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Transportverschlüsselung (TLS, SSL, etc.)	Richtlinie zur Klassifizierung und Handhabung von Informationen
E-Mail-Verschlüsselung	Richtlinie „Umgang mit mobilen Datenträgern“
Einsatz von VPN	Umsetzung des „Need-to-Share“ Prinzips
Nutzung geeigneter Protokolle wie sftp, https, etc.	
Einsatz geeigneter Verschlüsselungsalgorithmen	
Nutzung von Signaturverfahren	

6 Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in Verarbeitungssysteme eingegeben oder verändert worden sind.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Systemabhängige technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Genehmigungsverfahren für Rechtevergabe, -änderung, -entzug
Anmeldeprotokollierung	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

7 Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Feuerlöscher vor Serverraum	Regelmäßige Penetrationstest
Serverraumüberwachung: Temperatur, Feuchtigkeit, CO2	Notfallplan/regelmäßige DR-Tests
Redundante Klimatisierung im Serverraum	Wiederanlaufkonzept (Maßnahmen zur Wiederherstellung der Verfügbarkeit bei Systemausfall)
Redundante Rechenzentren und Infrastruktur	
Backups über mehrere Standorte	
Patchmanagement	
USV pro Rechenzentrum	
Lastenausgleich (Load-Balancing)	
Monitoring	
Geeignete Maßnahmen zum Schutz vor Schadsoftware	

8 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Bestellung internen Datenschutzbeauftragten
Zentrale Bereitstellung aller datenschutzrelevanten Informationen und Dokumentationen (Verfahren, Prozesse, Richtlinien etc.) für alle Beschäftigten der SVA (u.a. internes Wiki)	Verpflichtung und Belehrung aller Beschäftigten zur Einhaltung der Datenschutzbestimmungen, des Datengeheimnisses, der Vertraulichkeit und Geheimhaltung und anderer gesetzlicher Verschwiegenheits- und Geheimhaltungspflichten (u.a. GeschGehG, 203 StGB, TTDSG, etc.)
Datenbankgestütztes Verfahrensverzeichnis gem. Art. 30 DSGVO, indem alle Verarbeitungsvorgänge, für die SVA als Verantwortlicher oder Auftragsverarbeiter dokumentiert und soweit erforderlich bewertet werden.	Regelmäßige Sensibilisierung und Schulung der Beschäftigten (mindestens jährlich) zudem zusätzliche, bereichspezifische und anlassbezogene Maßnahmen
	Etablierter Prozess zur Durchführung von Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt gem. Art. 35 DSGVO)
	Etablierter Prozess zur Erfüllung der Transparenzpflichten ggü. den Betroffenen - die SVA kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	Aufbau und Organisation des internen Datenschutzes gem. dem Leitbild des BvD eV. mitsamt klarer Rollenverteilung zwischen der Datenschutzabteilung (Datenschutzkoordinatoren und -Leitung) und DSB
	Dokumentierter und implementierter Prozess zur Bearbeitung von Betroffenenanfragen
	Etablierte Datenschutzpolitik und Datenschutz-konzept
	Regelmäßige Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (Audit)
	Regelmäßige Überprüfung der Umsetzung des Datenschutzes in der SVA und Tätigkeitsbericht durch den DSB
	Initiale und anschließende regelmäßige Überprüfung eingesetzter Auftragsverarbeiter auf Datenschutzkonformität
	Dokumentation eines Löschkonzeptes für die Auftragsverarbeitung

9 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
Intrustion Prevention System (IPS)	Dokumentierter Prozess zur Erkennung, Bearbeitung und fristgerechten Meldung von (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörden) Auftraggeber (Verantwortlichen) und Betroffenen
Security Operations Center (SOC)	Einbindung von Datenschutz und Informationssicherheit in Sicherheitsvorfälle und Datenpannen/Datenschutzvorfälle
Internes Incident-Response-Team	Dokumentation von Sicherheitsvorfällen und Datenpannen/Datenvorfällen Notfallkonzept und -Prozess mit 24x7 besetztem Notfallverteiler zur Entgegennahme und Bearbeitung von Notfällen

10 Datenschutzfreundliche Voreinstellungen

Privacy by design/Privacy by default.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Begrenzungen von Systemen/Softwarelösungen zur Beschränkung der Eingabe von Daten. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind Technische Maßnahmen, die sicherstellen, dass Einwilligungen genauso einfach widerrufen wie abgegeben werden können Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können (anwendungsfallabhängig)	Frühzeitige Einbeziehung des Datenschutzteams in Produktentwicklung

11 Auftragskontrolle (Outsourcing an Dritte)

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln Regelung zur Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis und andere relevante Geheimhaltungs- und Verschwiegenheitspflichten Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter Regelung zum Einsatz weiterer Auftragsverarbeiter Initiale und anschließende regelmäßige Überprüfung eingesetzter Auftragsverarbeiter auf Datenschutzkonformität Sorgfältige Auswahl von Auftragsverarbeitern (insbesondere mit Bezug auf hinreichende Garantien zum Datenschutz und Datensicherheit) Übermittlung personenbezogener Daten in Drittländer nur unter Einhaltung geeigneter Garantien gem. Art. 44 ff. DSGVO und ggf. Durchführung von Transfer Impact Assessments (TIA)

12 Informationssicherheitspolitik

Technische Maßnahmen	Organisatorische Maßnahmen
Softwaregestütztes Informationssicherheits-Managementsystem (ISMS)	Internen Informationssicherheitsbeauftragten
Ticketsystem zur Bearbeitung von Informationssicherheitsvorfällen und -meldungen	Dokumentierter Prozess zur Erkennung, Bearbeitung und Meldung von Informationssicherheitsvorfällen
	Informationssicherheitsmanagement-System
	Regelmäßige Sensibilisierungen und Schulungen der Beschäftigten zur Informationssicherheit
	Eigenerklärung zur Informationssicherheit
	Leitlinien für den internen IT-Betrieb
	Etablierte Informationssicherheits-Richtlinien
	Regelmäßige interne Audits

13 Qualitätsmanagementpolitik

Technische Maßnahmen	Organisatorische Maßnahmen
Vollständige Prozesslandkarte der SVA	Interne Qualitätsmanagementbeauftragte
	Dokument zur Qualitätspolitik
	Qualitätsmanagementsystem
	Regelmäßige interne Audits

14 Zertifikate

Zertifizierung nach ISO 27001:2013 (ISMS)
Zertifizierung nach TISAX
Zertifizierung nach ISO 9001:2015
Zertifizierung nach ISO 14001:2015

ANHANG IV – LISTE DER UNTERAUFTRAGSVERARBEITER

Die SVA nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers grundsätzlich keine Leistungen von Externen in Anspruch. Abweichend davon können sich die Parteien bereits während der Angebotsphase über den Einsatz weiterer Parteien (z.B. Subunternehmer etc.) einigen, wodurch der Auftraggeber dessen Einsatz (soweit datenschutzrechtlich relevant) als Unterauftragsverarbeiter im Sinne diese Vertrages zustimmt. Eine aktualisierte Liste gem. diesen Anhangs IV wird auf Anfrage zur Verfügung gestellt.

Sollte die SVA zu einem späteren Zeitpunkt Unterauftragsverarbeiter hinzuziehen, werden die Parteien die vorliegende Vereinbarung zur Auftragsverarbeitung und Anlage IV entsprechend anpassen oder durch eine Individualvereinbarung ersetzen.

ANHANG V – LISTE VON VERBUNDENEN UNTERNEHMEN

Der Verantwortliche bzw. Auftraggeber genehmigt, dass folgende dem Verantwortlichen zugehörigen Unternehmen gem. Klausel 11.3 dieses Vertrages auf Basis dieses Vertrages den Auftragnehmer bzw. Auftragsverarbeiter direkt beauftragen dürfen:

Firma	Anschrift (inkl. Land)	Hinzugefügt am (Datum):	Ggf. Kontaktdaten einer Kontaktperson
zzt. keine	-	-	-