Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Diese Vereinbarung gilt zwischen dem jeweiligen Vertragspartner (Kunde) der SVA, in dessen Funktion als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO[1] und welcher nachstehend als „Auftraggeber“ bezeichnet wird. Verantwortlicher bezeichnet die natürliche oder juristische Person, Behörde oder sonstige Körperschaft, die allein oder gemeinsam mit anderen den Zweck und die Mittel der Verarbeitung personenbezogener Daten bestimmt. Für Fälle, in denen der Auftraggeber als Auftragsverarbeiter für einen anderen Verantwortlichen fungiert, gilt er im Sinne dieses Vertrags im Verhältnis zu SVA als eigenständiger Verantwortlicher.

Als Auftragnehmer in Ihrer Funktion als Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO, nachstehend „Auftragnehmer“ oder „SVA“ genannt, gilt die SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden.

Mit Beauftragung der SVA durch den Auftraggeber schließen die Parteien diesen Vertrag zur Auftragsverarbeitung.

Anwendungsbereich

Diese Vereinbarung erstreckt sich 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

Diese Vereinbarung kann jederzeit durch eine, zwischen den Parteien verhandelte, Individualvereinbarung (z. B. Rahmenvertrag zur Auftragsverarbeitung)[2] 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 besteht, hat diese Anwendungsvorrang gegenüber dieser Vereinbarung. Die Zuordnung zwischen der jeweiligen beauftragten Leistung und des zugehörigen Vertrages zur Auftragsverarbeitung wird durch die SVA im Verarbeitungsverzeichnis gem. Art 30 DSGVO dokumentiert.

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).

[2] Durch den Rahmenvertrag zur Auftragsverarbeitung (RAV) kann eine Vielzahl von IT-Dienstleistungen pauschal legitimiert werden, ohne dass für jede Leistung eine Einzelvereinbarung geschlossen werden muss. Dies kann unter Datenschutz@SVA.de angefordert werden.

Inhaltsverzeichnis

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den vereinbarten Leistungen ergeben. Daher ist die korrespondierende Leistungsvereinbarung Bestandteil dieser Vereinbarung. Der Anwendungsbereich erstreckt sich auf alle Tätigkeiten, die mit den vereinbarten Leistungen in Verbindung stehen und die Verarbeitung personenbezogener Daten des Auftraggebers durch den Auftragnehmer zum Gegenstand haben. Die Vereinbarung zur Auftragsverarbeitung geht nur hinsichtlich der datenschutzrechtlichen Regelungen der Leistungsvereinbarung vor. Für Rechtsnormverweise und deren Begrifflichkeiten in dieser Vereinbarung gelten die jeweiligen, zum Vertragsschluss, aktuellen Fassungen oder deren entsprechende Nachfolgeregelungen.

1. Auftragsgegenstand sowie Art und Zweck der Verarbeitung

(1) Der Auftrag des Auftraggebers an den Auftragnehmer umfasst Arbeiten und/oder Leistungen, die sich aus der jeweils korrespondierenden Leistungsvereinbarung (z. B. Angebot mit Annahme, Hauptvertrag, Kontingent-/Einzelabruf, EVB-IT, Werk-/Dienstleistungsvertrag, Leistungsvertrag etc.) ergeben. Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen Vertragszwecke.

(2) Sofern die Dienstleistungserbringung mit Unterstützung von Unterauftragnehmern (siehe Nr. 13 dieses Vertrags sowie Anlage) avisiert ist, erfasst der Auftragnehmer unter anderem die zugehörige Leistungsvereinbarung mitsamt Auftragsgegenstand, Zweck, Art der personenbezogenen Daten, Dauer sowie die Unterauftragnehmer im Verzeichnis der Verarbeitungstätigkeiten.

2. Dauer der Verarbeitung und Vertragslaufzeit

Die Dauer der Verarbeitung und Laufzeit dieser Vereinbarung entspricht der Dauer der korrespondierenden, vereinbarten Leistung gem. Nr. 1 Abs. 1 dieser Vereinbarung.

3. Art der personenbezogenen Daten

(1) Von der Datenverarbeitung betroffene Arten personenbezogener Daten ergeben sich aus der jeweiligen zugehörigen Leistungsvereinbarung und umfassen prinzipiell sämtliche Datenarten, die auf den Systemen des Auftraggebers verarbeitet werden und die im Rahmen der Leistungsvereinbarung im Zugriffsbereich der SVA-beschäftigten Personen stehen.

(2) Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Arten personenbezogener Daten kann die Datenverarbeitung folgende Arten umfassen:
- Stammdaten (Name, Adresse, E-Mail, Tel.-Nr., IP-Adresse etc.),
- Ordnungsdaten (Kunde-Nr., Mitarbeiter-Nr., Mitglieds-Nr. etc.),
- besondere Arten von personenbezogenen Daten (Art. 9 DSGVO),
- Finanz-/Mahndaten, Privatgeheimnisse (§ 203 StGB),
- Ergebnisse automatisierter Entscheidungen (Scoring etc.),
- Daten aus Keylogger (z. B. bestimmte Data-Loss-Prevention Systeme),
- Telekommunikationsdaten (§ 3 TTDSG),
- weitere sensible Daten ohne Personenbezug (Geschäftsgeheimnis (§ 2 GeschGehG)).

(3) Der Auftraggeber hat dem Auftragnehmer von den in Nr. 3 Abs. 2 abweichende personenbezogene Daten mitzuteilen. Die in dieser Mitteilung aufgeführte Anpassung der personenbezogenen Daten werden als Ergänzung ein Bestandteil dieser Vereinbarung. Soweit nicht anders vereinbart, gelten die Bestimmungen dieses Vertrages zur Auftragsverarbeitung entsprechend.

4. Kategorien betroffener Personen

(1) Konkretisierend, abweichend oder ergänzend zu den in der Leistungsvereinbarung definierten Kategorien betroffener Personen, kann die Datenverarbeitung prinzipiell sämtliche Personenkategorien umfassen, die durch die vereinbarte Leistung verarbeitet werden. Dies beinhaltet:
- beschäftigte Personen des Auftraggebers i.S.d. § 26 BDSG,
- Endkunden/Kunden des Auftraggebers,
- Lieferanten des Auftraggebers,
- Sonstige (Bürgen, andere Dritte, wie Steuerberater etc.).

(2) Der Auftraggeber hat dem Auftragnehmer von den in Nr. 4 Abs. 1 abweichende Kategorien betroffener Personen mitzuteilen. Die in dieser Mitteilung aufgeführte Anpassung der Kategorien betroffener Personen werden als Ergänzung ein Bestandteil dieser Vereinbarung. Soweit nicht anders vereinbart, gelten die Bestimmungen dieses Vertrages zur Auftragsverarbeitung entsprechend.

5. Datenschutzbeauftragte der Vertragsparteien

(1) Jede Vertragspartei, die gesetzlich zur Benennung eines Datenschutzbeauftragten verpflichtet ist, gibt zum Zwecke der Abstimmung in datenschutzrechtlichen Fragen die Kontaktinformationen des benannten Datenschutzbeauftragten weiter. Im Falle, dass keine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht, ist eine gleichgestellte Ansprechperson mitzuteilen.

(2) Datenschutzbeauftragter SVA

Vorname Name	Michael Neunaber
Funktion/ Firma	Datenschutzbeauftragter SVA System Vertrieb Alexander GmbH (DSB SVA)
Adresse	Borsigstraße 26, 65205 Wiesbaden
Telefon	+49 151 18027863
E-Mail	datenschutz@sva.de

6. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird Daten des Auftraggebers nur zur Erfüllung der vertraglich vereinbarten Leistungen und nach Weisung des Auftraggebers verarbeiten.

(2) Weisungen erfolgen durch den Auftraggeber in Schriftform oder Textform (bspw. per E-Mail).

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Meinung ist, dass eine Weisung des Auftraggebers gegen geltende datenschutzrechtliche Vorschriften oder die vertraglichen Vereinbarungen verstößt.

7. Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten nach DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer hat, sofern gesetzlich vorgeschrieben, einen Datenschutzbeauftragten zu bestellen. Änderungen an dessen Kontaktdaten, wie in Nr. 5 dieses Vertrags angegeben, werden dem Auftraggeber unverzüglich mitgeteilt.

b) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Personen ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu auftragsrelevanten personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers, einschließlich der in diesem Vertrag eingeräumten Befugnisse, verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Bei vorliegender gesetzlicher Verpflichtung zur Verarbeitung besteht vor der Verarbeitung eine Mitteilungspflicht des Auftragnehmers gegenüber dem Auftraggeber, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

c) Der Auftragnehmer gewährleistet anhand des Schutzbedarfs die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen.

d) Der Auftragnehmer und der Auftraggeber arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Der Auftragnehmer gewährleistet das unverzügliche Informieren des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Verlangt eine betroffene Person die Herausgabe bzw. die Bekanntgabe von Daten, die im Rahmen der Auftragsverarbeitung erhoben, verarbeitet oder genutzt werden, leitet der Auftragnehmer das diesbezügliche Begehren an den Auftraggeber weiter.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person.

i) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber ist sicherzustellen.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung oder Übermittlung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorheriger Konsultation. Hierzu gehören u. a. die:

a) Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und

Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,

b) Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
c) Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen,
d) Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Änderung, Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers ändern, berichtigen, löschen oder deren Verarbeitung einschränken.

(2) Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Vertraulichkeit und Geheimhaltung

(1) Der Auftragnehmer ist verpflichtet, seine Beschäftigten und Erfüllungsgehilfen, die an der Verarbeitung personenbezogener Daten oder anderer vertraulicher oder geheimhaltungsbedürftiger Informationen beteiligt sind, gemäß den entsprechenden gesetzlichen Vorschriften (u. a. § 3 TTDSG, § 53 BDSG, § 203 StGB, § 2 GeschGehG, § 39 PostG) dokumentiert zu belehren und zu verpflichten. Belehrung und Verpflichtung bestehen auch nach Beendigung der Tätigkeit fort.

(2) Informationen im Sinne der Nr. 9 Abs. 1 dieses Vertrags sind u. a. alle mündlichen, schriftlichen und sonstigen Informationen, Unterlagen, Datenträger, anderes Material und Software, die auf die jeweilige Partei bezogene Tatsachen, Umstände und Vorgänge oder technisches Wissen der jeweiligen Partei enthalten.

(3) Die Informationen dürfen nur zu den in den Leistungsvereinbarungen vereinbarten Vertragszwecken verwendet werden. Sie dürfen nur dann an Dritte weitergegeben werden, wenn die Weitergabe dem Vertragszweck dient oder legitim eingefordert wird und die Dritten vor Weitergabe zur Vertraulichkeit und Geheimhaltung verpflichtet wurden. Bei Beendigung dieses Vertrages oder auf schriftliche Anforderung einer Partei wird die andere Partei die Informationen nicht mehr verwenden.

(4) Die Pflichten des Auftragnehmers zur Vertraulichkeit und Geheimhaltung sind auch auf jegliche Unterauftragnehmer gemäß Nr. 13 dieses Vertrags anzuwenden.

(5) Ausnahmen der Vertraulichkeit und Geheimhaltungspflicht sind Fälle, in denen

a) eine Offenlegung zwingend erforderlich ist (z. B. auf Grund eines gerichtlichen oder behördlichen Verfahrens) oder
b) die Informationen bereits öffentlich oder anderweitig bekannt waren oder
c) die zur Vertraulichkeit und Geheimhaltung verpflichtete Partei rechtmäßig von Dritten ohne Vorbehalt erhalten hat oder
d) offensichtlich kein Interesse an einer Vertraulichkeit oder Geheimhaltung besteht.

(6) Weitere Ausnahmen bedürfen der ausdrücklichen Zustimmung derjenigen Partei, deren Informationen betroffen sind.

10. Sicherheit der Verarbeitung

(1) Der Auftragnehmer hat die Sicherheit der Datenverarbeitung gem. Art. 28 Abs. 3 lit. c DSGVO i.V.m. Art. 30 Abs. 2 (Verzeichnis von Verarbeitungstätigkeiten) und 32 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

(2) Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind durch diesen in schriftlicher Form zu dokumentieren. Die Dokumentation ist dieser Vereinbarung als Anlage beizufügen. Ändern sich die gesetzlichen Anforderungen an die technischen und organisatorischen Maßnahmen, ist der Auftragsverarbeiter verpflichtet, seine technischen und organisatorischen Maßnahmen an diese neuen gesetzlichen Anforderungen anzupassen.

(3) Bei Leistungserbringung in den Räumen des Auftraggebers, können über diese Regelungen hinaus Verhaltensregeln, im Sinne von technischen und organisatorischen Maßnahmen, für Mitarbeiter fremder Unternehmen vereinbart werden.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

11. Kontrollrechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, Überprüfungen zur Sicherstellung einer auftrags- und weisungskonformen Datenverarbeitung durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, sofern diese nicht in einem Wettbewerbsverhältnis mit dem Auftragnehmer stehen oder andere berechtigte Gründe seitens des Auftragnehmers dem entgegenstehen. Jede Partei hat die dabei für sich selbst anfallenden Kosten selbst zu tragen. Das Vorgehen sowie Art und Umfang der Kontrollen sind im Vorfeld rechtzeitig durch Auftraggeber und Auftragnehmer einvernehmlich abzustimmen und möglichst ohne Störung des Betriebsablaufes durchzuführen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Als Grundlage für die Prüfung der technischen und organisatorischen Maßnahmen durch den Auftraggeber können zusätzlich zu der vom Auftragnehmer bereitgestellten Dokumentation dienen:

a) Der Prüfungsbericht oder das Zertifikat einer vom Auftragnehmer beauftragten und von einem unabhängigen Sachverständigen bzw. dem bestellten Datenschutzbeauftragten durchgeführten Datenschutzprüfung.

b) Die vom Auftraggeber erstellte Prüfungsdokumentation einer von ihm beim Auftragnehmer durchgeführten Prüfung, wenn der Auftragnehmer keine Prüfung oder Zertifizierung beauftragt hat.

(4) Der Nachweis entsprechender Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.

(5) Sofern sich aus der vom Auftraggeber durchgeführten Prüfung notwendige Änderungsbedarfe an den technischen und organisatorischen Maßnahmen ergeben, werden diese in Abstimmung zwischen Auftraggeber und Auftragnehmer durch den Auftragnehmer umgesetzt.

12. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Sofern keine gesetzliche Vorschrift eine über das Vertragsende hinausgehende Aufbewahrung der Daten vorschreibt, wird der Auftragnehmer, die mit diesem Vertragsverhältnis im Zusammenhang stehenden Daten in seinen Datenverarbeitungsanlagen löschen. Auf Wunsch des Auftraggebers werden diese Daten vor der Löschung elektronisch an den Auftraggeber übergeben.

13. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche (IT-)Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Reinigungsservices und Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der eigenen Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme, vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. (IT-)Dienstleistungen stellen insofern nur dann ein Unterauftragsverhältnis dar, wenn sie im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden.

(2) Die Absicht des Auftragnehmers zur Beauftragung eines auftragsrelevanten Unterauftragsverhältnisses ist dem Auftraggeber schriftlich oder in Textform anzuzeigen. Der Auftraggeber erhält dadurch die Gelegenheit, Einspruch gegen die Hinzuziehung oder die Ersetzung des jeweiligen Unterauftragnehmers zu erheben, der Einsatz eines Subunternehmers darf jedoch nicht weder Treu und Glauben verweigert und muss begründet werden.

(3) Der Auftragnehmer hat den Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln.

(4) Der Auftragnehmer hat bereits bei der Beauftragung eines Unterauftragsverarbeiters sicherzustellen, dass alle in diesem Vertrag vereinbarten Regelungen und bestehende ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragsverarbeiter gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragsverarbeiter einen Auftragsverarbeitungsvertrag zu schließen, der die Anforderungen aus Art. 28 DSGVO erfüllt.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des Auftraggebers und der Aufsichtsbehörden auch gegenüber dem Unterauftragsverarbeiter gelten. Es ist insbesondere vertraglich zu regeln, dass der Unterauftragsverarbeiter diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen, insbesondere unter Berücksichtigung der Vorgaben die sich aus den Art. 44 ff. DSGVO ergeben, sicher. Gleiches gilt, wenn Dienstleister im Sinne von Nr. 13 Abs. 1 dieses Vertrags eingesetzt werden sollen.

14. Haftung

(1) Die an der Verarbeitung personenbezogener Daten beteiligten Parteien haften gemäß den vertraglichen Vereinbarungen, gesetzlichen Regelungen und Vorschriften der DSGVO.

(2) Haftungsbeschränkungen anderer vertraglicher Regelungen zwischen den Vertragsparteien sind in Bezug auf diese Vereinbarung nicht anzuwenden.

(3) Der Rechtsweg bleibt unberührt.

15. Sonstige Informationspflichten, Schriftformklausel, Rechtswahl

(1) Die Rechtswahl bestimmt sich vorrangig nach der Regelung der jeweiligen Leistungsvereinbarung oder den angewendeten AGB. Ist dort keine Rechtswahl getroffen, gilt deutsches Recht und der Gerichtsstand ist Wiesbaden.

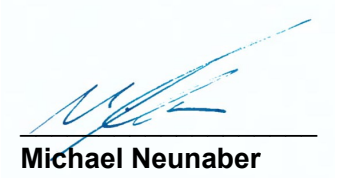
(2) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber darüber zu informieren. Der Auftragnehmer wird alle in

diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Änderungen und Ergänzungen dieses Vertrags und aller Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – 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.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.



Michael Neunaber
Datenschutzbeauftragter der SVA

Anlage Sicherheit der Verarbeitung

Durch die SVA wurden die nachfolgend dokumentierten, technischen und organisatorischen Schutzmaßnahmen getroffen. Auftragnehmer und Unterauftragnehmer können 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 Anhang zu dieser Vereinbarung nicht ersichtlich ist, gelten die nachfolgenden technischen und organisatorischen Schutzmaßnahmen als vom Auftragnehmer erfüllt.

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 trifft die SVA geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere 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 wurden.

1. Pseudonymisierung

Personenbezogene Daten des Verantwortlichen können auf dessen Weisung in einer Weise verarbeitet werden, sodass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die eine unbefugte Identifizierung der betroffenen Person ausschließen.

2. Maßnahmen zur Verschlüsselung

- Verschlüsselte Aufbewahrung von Passwörtern
- Gesicherte Datenweitergabe (z. B. FTPS, TLS)
- Gesichertes WLAN

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. *Maßnahmen, durch die Unbefugten der Zutritt verwehrt wird:*

- Türsicherungen (elektrische Türöffner, Zahlenschloss)
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Spezielle Schutzvorkehrungen des Serverraums
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- Nicht-reversible Vernichtung von Datenträgern
- Besucherregelung (Abholung am Empfang, Begleitung nach dem Besuch bis zum Ausgang)

b. *Maßnahmen, die verhindern, dass Unbefugte die Verarbeitungssysteme nutzen können:*

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Begrenzung der befugten Benutzer
- Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- Firewall

c. *Maßnahmen, die gewährleisten, dass nur berechtigte Personen auf die Verarbeitungssysteme zugreifen und personenbezogene Daten nicht unbefugt lesen, kopieren, verändern oder entfernen können:*

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Auswertungen/Protokollierungen von Datenverarbeitungen
- Autorisierungsprozess für Berechtigungen
- Genehmigungsroutinen
- Profile/Rollen
- Funktionstrennung „Segregation of Duties"
- Nicht-reversible Löschung von Datenträgern

d. *Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:*

- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen

4. Maßnahmen zur Sicherstellung von Integrität

- Zugriffsrechte
- Systemseitige Protokollierungen
- Dokumenten Management System (DMS) mit Änderungshistorie
- Sicherheits-/Protokollierungssoftware
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Protokollierung von lesenden Zugriffen
- Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

- Sicherheitskonzept für Software- und IT-Anwendungen
- Back-Up Verfahren
- Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Spiegeln von Festplatten
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- Brand- und/oder Löschwasserschutz des Serverraums
- Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- Klimatisierter Serverraum
- Virenschutz
- Firewall
- Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

6. Maßnahmen zur Sicherstellung der Belastbarkeit

- Redundante Stromversorgung
- Ausreichende Kapazität von IT-Systeme und Anlagen
- Logistisch gesteuerter Prozess zur Verhinderung von Leistungsspitzen
- Redundanten Systeme/Anlagen
- Resilienz und Fehler-Management

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Verfahren für regelmäßige Kontrollen/Audits
- Konzept für regelmäßige Überprüfung, Bewertung und Evaluierung

8. Weisungskontrolle/Auftragskontrolle

- Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpersonen
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter
- Verpflichtung aller Mitarbeiter zur Vertraulichkeit
- Benennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DSGVO: Als interner Datenschutzbeauftragter ist Michael Neunaber (SVA System Vertrieb Alexander GmbH, Borsigstraße 26, 65205 Wiesbaden, datenschutz@sva.de, mobil: +49 151 18027863, Fax.: 06211/536-399) benannt.
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO
- Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
- Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Sicherheit der Verarbeitung
- Prozess zur Weiterleitung von Betroffenenanfragen.

Anlage Unterauftragsverarbeiter

Die SVA nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers keine Leistungen von Externen in Anspruch.

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