

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Vorbemerkungen

- (1) Der Auftragnehmer bietet mit dem Produkt „s3:connect“ („**s3:connect**“) als Software-as-a-Service eine digitale Lösung zum webbasierten Management flexibler Arbeitsumgebungen an. Er hostet und pflegt s3:connect unter Einschaltung seines Entwicklungs- und Hostingpartners Cancom Austria AG.
- (2) Bei der Erbringung der Dienstleistungen werden der Auftragnehmer und ggf. eingeschaltete weitere Dienstleister Zugriff auf von dem Auftraggeber zugänglich gemachte personenbezogene Daten erhalten und solche Daten verarbeiten.
- (3) Die Vertragspartner schließen daher zur Einhaltung der in diesem Zusammenhang zu beachtenden datenschutzrechtlichen Anforderungen die vorliegende Vereinbarung zur Auftragsverarbeitung im Sinne von Art. 28 DSGVO. Im weiteren Verlauf wird übergreifend Bezug auf die Art. 28 DSGVO genommen.

§ 1 Begriffsdefinitionen

Für diesen Vertrag gelten hinsichtlich aller gesetzlich definierten Begriffe die Begriffsdefinitionen der DSGVO. Soweit nachfolgend von „Daten“ die Rede ist, sind damit personenbezogene Daten im Sinne dieser Vereinbarung und der DSGVO gemeint.

§ 2 Gegenstand dieser Vereinbarung zur Auftragsverarbeitung

- (1) Der Auftragnehmer erbringt im Auftrag des Auftraggebers die in dem/den gesondert geschlossenen Leistungsschein(en) s3:connect und den Allgemeinen Vertrags- und Lizenzbedingungen s3:connect (im Folgenden zusammen „**Hauptvertrag**“) geregelten Leistungen. Danach können der Auftraggeber und seine Mitarbeiterinnen und Mitarbeiter mithilfe von s3:connect und ggf. eingesetzter Drittkomponenten z.B. in Open Space-Bereichen verfügbare Büroarbeitsplätze und -räume per Smartphone oder anderen Devices ermitteln, buchen und verwalten.
- (2) Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers,

sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag sowie aus der **Anlage 1** zu dieser Vereinbarung. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

- (3) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen, soweit datenschutzrechtlich relevant, im Zweifel den Regelungen des Hauptvertrags vor.
- (4) Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.
- (5) Die Laufzeit dieser Vereinbarung richtet sich nach § 11.
- (6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland außerhalb des genannten Gebiets bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 3 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierte Art personenbezogener Daten des ebenfalls in **Anlage 1** näher spezifizierten Kreises betroffener Personen. Diese Daten umfassen keine besonderen Kategorien personenbezogener Daten.

§ 4 Weisungsrecht

- (1) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
- (2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (nachfolgend auch „**Einzelweisung**“). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Einzelweisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigte(n) Person(en) des Auftraggebers und die zum Empfang von Weisungen bei dem Auftragnehmer zuständige(n) Person(en) ergeben sich aus **Anlage 2**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.
- (3) Alle erteilten Einzelweisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Einzelweisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Dadurch verursachte Mehraufwände des Auftragnehmers hat der Auftraggeber nach Maßgabe der in **Anlage 3** geregelten Tages- bzw. Stundensätze des Auftragnehmers zu vergüten.
- (4) Ist der Auftragnehmer der Ansicht, dass eine Einzelweisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, so hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Einzelweisung ablehnen.

§ 5 Schutzmaßnahmen des Auftragnehmers

- (1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und Unterlagen und Daten gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 4** aufgeführten Maßnahmen getroffen hat. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Der beim Auftragnehmer bestellte betriebliche Datenschutzbeauftragte ist in **Anlage 5** genannt.

- (3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrags beauftragt werden (im Folgenden „**Beschäftigte**“), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.
- (4) Sollten Daten, die Gegenstand dieses Vertrags sind, durch Mitarbeiter oder Mitarbeiterinnen des Auftragnehmers oder eingeschalteter Dienstleister im

Homeoffice verarbeitet werden, so wird der Auftragnehmer besondere, für den Schutz der personenbezogenen Daten und die Einhaltung der Bestimmungen dieses Vertrags und der Vorgaben der DSGVO geeignete und von den Mitarbeitern und Mitarbeiterinnen zu beachtende Richtlinien festlegen und ggf. eingeschaltete Dienstleister in im Wesentlichen gleicher Weise verpflichten.

§ 6 Informationspflichten des Auftragnehmers

- (1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:
 - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
 - b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
 - c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.
- (3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

- (4) Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DSGVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DSGVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DSGVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 4 dieses Vertrags durchführen.
- (5) 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 unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.
- (6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.
- (7) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- (8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.
- (9) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.
- (2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.
- (3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.
- (4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.
- (5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 5 Abs. 4 auf Verlangen nach.
- (6) Der Auftraggeber vergütet dem Auftragnehmer den Aufwand, der ihm im Rahmen der Kontrolle entsteht, gemäß dem im Hauptvertrag verabredeten Satz.

§ 8 Einsatz von Subunternehmern

- (1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 6** genannten Subunternehmer durchgeführt.
- (2) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern (im Folgenden „**Subunternehmerverhältnis**“) befugt. Der Auftragnehmer informiert den Auftraggeber stets über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter (vgl. Art. 28 Abs. 2 Satz 2 DSGVO). Der Auftraggeber erhält hierdurch die Möglichkeit, innerhalb eines Monats nach Erhalt der Information gegen die Änderung Einspruch einzulegen. Sollte ein Einspruch konkrete Anhaltspunkte dafür ergeben, dass die beabsichtigte Änderung keine Gewähr für die ordnungsgemäße Datenverarbeitung im Sinne von Art. 28 DSGVO bietet oder sonst gegen rechtliche Anforderungen verstößt, so wird der Auftragnehmer von der jeweiligen Änderung absehen.
- (3) Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.
- (4) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-

Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

- (1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie 32 und 36 DSGVO.
- (2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 10 Haftung

- (1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.
- (2) Sollte der Auftragnehmer aufgrund eines von dem Auftraggeber zu vertretenden Verstoßes gegen diese Vereinbarung oder gegen datenschutzrechtliche Bestimmungen von einem Dritten in Anspruch genommen oder sollte ein Bußgeld gegenüber dem Auftragnehmer verhängt werden, so wird der Auftraggeber den Auftragnehmer entsprechend dem Anteil seiner Verantwortung freistellen und ihm durch die Inanspruchnahme entstehende Aufwendungen und Schäden ersetzen. Eine weitergehende Haftung des Auftraggebers nach Maßgabe der gesetzlichen Bestimmungen bleibt unberührt, ebenso der gesetzliche Rückgriffsanspruch nach Art. 82 Abs. 5 DSGVO.
- (3) Sofern vorstehend nicht anders geregelt, haftet der Auftragnehmer nach Maßgabe der im Hauptvertrag vorgesehenen Haftungsbeschränkungen und -ausschlüsse. Diese gelten entsprechend auch im Falle eines Innenregresses gegenüber dem Auftragnehmer.

§ 11 Beginn und Ende der Verarbeitung

- (1) Die vorliegende Vereinbarung beginnt mit Unterzeichnung durch beide Parteien und endet, sofern nachfolgend nicht abweichend vereinbart, mit Beendigung des Hauptvertrags. Dieser Vertrag endet auch dann, wenn der Hauptvertrag in der Weise geändert wird, dass die dabei stattfindende Datenverarbeitung nicht mehr als Datenverarbeitung im Auftrag anzusehen ist. Falls mehrere Leistungsscheine über die Nutzung von s3:connect bestehen, endet der Vertrag erst mit dem letzten noch bestehenden Leistungsschein.
- (2) Jede Partei kann den vorliegenden Vertrag nach den im Hauptvertrag geregelten Bestimmungen ordentlich kündigen. Falls die Parteien in diesem Fall nicht zugleich den Hauptvertrag kündigen, werden sie zugleich eine neue, den datenschutzrechtlichen Anforderungen ebenfalls entsprechende Vereinbarung zur Auftragsverarbeitung schließen.
- (3) Das Recht eines jeden Vertragspartners, den vorliegenden Vertrag aus wichtigem Grund fristlos zu kündigen, bleibt unberührt. § 11 Abs. (2) Satz 2 gilt entsprechend.
- (4) Kündigungen sind nur wirksam, wenn sie schriftlich oder in Textform erklärt wurden.

§ 12 Beendigung des Hauptvertrags

- (1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger mit Bezug zu personenbezogenen Daten im Sinne dieser Vereinbarung zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.
- (2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

- (3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

- (1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.
- (2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- (3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
- (4) Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts und der Kollisionsregeln des internationalen Privatrechts.
- (5) Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz von Sedus, wenn der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder keinen allgemeinen Gerichtsstand im Inland hat. Jede Partei ist unabhängig davon berechtigt, die andere Partei an deren allgemeinem Gerichtsstand zu verklagen.

§ 14 Anlagen

Folgende Vertragsanlagen sind Vertragsbestandteil:

Anlage 1 Umfang und Zweck der Verarbeitung; Kategorien von Betroffenen und Arten von Daten

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 1

Umfang und Zweck der Verarbeitung; Kategorien von Betroffenen und Arten von Daten

Umfang und Zweck der Verarbeitung

Die vom Auftragnehmer als Software-as-a-Service bereitgestellte se:connets Software unterstützt das webbasierte Management flexibler Arbeitsumgebungen. Mit Hilfe dieser Software können nach näherer Maßgabe des Hauptvertrags z.B. in Open Space-Bereichen verfügbare Büroarbeitsplätze und Besprechungsräume per Smartphone oder anderen Devices ermittelt, gebucht und verwaltet werden. Außerdem könnten Mitarbeiter*innen aufgefunden werden, die z.B. an gemeinsamen Projekten arbeiten und dafür passende Plätze und Räume gebucht haben. Die durch die jeweils nutzungsberechtigten Personen angegebenen personenbezogene Daten werden zu diesen Zwecken verarbeitet.

Kategorien von Betroffenen

Es können bestimmungsgemäß personenbezogene Daten der Kategorien von Betroffenen für die oben genannten Zwecke erhoben und verarbeitet werden, die typischerweise Büroräume des Auftraggebers nutzen, insbesondere:

- Beschäftigte; Organe, Gesellschafter*innen und ggf. freie Mitarbeiter*innen des Auftraggebers und verbundener Unternehmen
- Beschäftigte; Organe, Gesellschafter*innen und ggf. freie Mitarbeiter*innen von Geschäftspartnern des Auftraggebers und verbundener Unternehmen
- Beschäftigte; Organe, Gesellschafter*innen und ggf. freie Mitarbeiter*innen von Dienstleistern des Auftraggebers und verbundener Unternehmen
- Gäste des Auftraggebers und verbundener Unternehmen.

Arten von Daten

Folgende Arten von Daten können bei bestimmungsgemäßer Nutzung typischerweise erhoben und verarbeitet werden:

- Vor- und Nachname

- E-Mail-Adresse, Telefonnummer
- Angaben zu gebuchten oder genutzten Büroarbeitsplätzen wie z.B. Postanschrift des Gebäudes des Unternehmens bzw. der Niederlassung o.Ä. sowie ggf. Gebäude-, Stockwerk-, Raum- und Büroarbeitsplatzbezeichnung.

Anlage 2

Technische und organisatorische Maßnahmen des Auftragnehmers (Art 32 Abs 1 DSGVO)

Der Auftragsverarbeiter hat die Datensicherheit bzw. ein dem Verarbeitungsrisiko angemessenes, dem Stand der Technik entsprechendes Schutzniveau hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie hinsichtlich der Belastbarkeit von Systemen zu gewährleisten. Um ein dem Stand der Technik stets entsprechendes Schutzniveau zu garantieren ist der Auftragsverarbeiter ISO 9001, ISO 20000 und ISO 27001 zertifiziert und bestrebt diese Zertifizierungen stets aufrecht zu erhalten.

Es wird festgehalten, dass sämtliche genannten Maßnahmen lediglich in den Betriebsräumlichkeiten und in der Zugriffssphäre des Auftragsverarbeiters gelten und umgesetzt wurden. Der Auftragsverarbeiter übernimmt keine Verantwortung und Haftung für die im Macht- und Einflussbereich des Verantwortlichen notwendigen und/oder geltenden technischen oder organisatorischen Maßnahmen. Insbesondere ausgenommen sind im Verantwortungsbereich des Verantwortlichen befindliche(s) Einrichtungen, Personal, IT-Infrastruktur, Gegenstände und Daten.

Soweit für die Vertragserfüllung relevant, sind dahingehend bereits (oder werden noch rechtzeitig) folgende Maßnahmen durch den Auftragsverarbeiter in seiner Systemumgebung gesetzt:

Zutrittskontrolle

- ✓ Personenkontrolle durch Portier oder Sicherheits-/Wachdienst
- ✓ Bewachung an Wochenenden/Feiertagen
- ✓ Alarmanlage/Einbruchmeldesystem
- ✓ Videoüberwachung der Zugänge
- ✓ Zugangsbeschränkung für Büro- und Geschäftsräume
- ✓ Sicherheitsschlösser
- ✓ Absicherung von Gebäudeschächten, Hintertüren, Nebeneingängen etc.
- ✓ Bewegungsmelder/Lichtschranken
- ✓ Chipkarten-/Transponderregelung
- ✓ Schlüsselregelung
- ✓ Manuelles Schließsystem
- ✓ Protokollierung von Schlüssel-/Chipkarten-/Transponderausgaben
- ✓ Generalschlüsselregelung
- ✓ Regelung des Besucherzutritts (Anmeldung, Protokollierung)
- ✓ Berechtigungsausweis-Tragepflicht

- ✓ Spezielle Sicherung/Zutrittsbeschränkung für Serverräume und Archive

Zugangskontrolle

- ✓ Sichere Aufbewahrung von Datenträgern
- ✓ „clean desk“ (digitaler Arbeitsplatz, Reinigung des virtuellen Desktops)
- ✓ Absicherung interner Schnittstellen (WLAN, Bluetooth etc.)
- ✓ Richtlinie zur Passwortsicherheit
- ✓ Berechtigungskonzept
- ✓ Erstellung von Benutzerprofilen
- ✓ Zuordnung von Benutzerprofilen zu Datenverarbeitungssystemen
- ✓ Authentifizierung über eindeutige User-ID
- ✓ Authentifizierung über Benutzername und Passwort bzw. Möglichkeit zur biometrischen Anmeldung
- ✓ Gesicherte Verbindung bei Fernwartung
- ✓ Protokollierung der Zugänge (An- und Abmeldung) zu Datenverarbeitungssystemen
- ✓ Kontosperrung bei fehlerhaften Zugangsversuchen
- ✓ Automatische Rechtersperre bei vorübergehender Abwesenheit
- ✓ Regelmäßiger erzwungener Passwortwechsel
- ✓ Unverzügliche Sperre der Berechtigung ausgeschiedener Benutzer
- ✓ Verwaltung der Rechte durch Systemadministrator
- ✓ Sichere Aufbewahrung des Administrator-Passworts
- ✓ Angriffserkennungssystem/Anti-Viren-Software sowie verhaltensbasierende Malware-Erkennung und Sandboxing
- ✓ Viren-Scanner für Server und Arbeitsplatzrechner
- ✓ Abschottung durch Firewall inkl. Intrusion Detection & Prevention System
- ✓ Daten-/Festplattenverschlüsselung von mobilen Endgeräten (Smartphone, Notebook, USB-Stick etc.)
- ✓ Einsatz von Schutzprogrammen und Administrationssoftware auf Smartphones und Tablet-PCs
- ✓ Verbot der nicht genehmigten Installation von Soft- und Hardware
- ✓ Regelmäßige Aktualisierung der Schutzprogramme (Updates etc.)

Zugriffskontrolle

- ✓ Zugriffsbeschränkung für Computersysteme und Netzlaufwerke auf berechtigte Benutzer
- ✓ Zugriffsbeschränkung für Backup-Datenträger auf Systemadministratoren
- ✓ Berechtigungskonzept
- ✓ Prozess zur Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen
- ✓ Berechtigungsminimierung nach Zweckbindungsprinzip
- ✓ Differenzierte Berechtigungen (Lesen, Ändern, Profile, Rollen, Transaktionen, Objekte)
- ✓ Berechtigungsverwaltung durch Systemadministrator
- ✓ Meldung und Auswertung erfolgter/versuchter Sicherheitsverletzungen
- ✓ Überschreibung der Datenträger mit geeigneter Software vor Wiederverwendung
- ✓ Ordnungsgemäße Datenträgervernichtung
- ✓ Einsatz geeigneter Datenschutzhälter zur Verhinderung unbefugter Entnahmen
- ✓ Protokollierung der Entsorgung von Daten (Vernichtungszertifikat etc.)
- ✓ Verschlüsselung von Datenträgern

Weitergabekontrolle

- ✓ Monitoring des Datenverkehrs
- ✓ Verschlüsselte programmgesteuerte Übermittlung von Daten
- ✓ Kryptografisches Verschlüsselungsverfahren (z. B. S/MIME)
- ✓ Datentransfer über gesicherte Verbindungen (z. B. https/SFTP)
- ✓ Protokollierung von Abruf- und Übermittlungsvorgängen
- ✓ Einrichtung von Standleitungen bzw. VPN-Verfahren (SD WAN)
- ✓ Einsatz von Passwörtern und Passwortsicherheit
- ✓ Getrennte Wege zur Passwortübermittlung

Eingabekontrolle

- ✓ Nachvollziehbarkeit der Zugriffe anhand individueller Benutzernamen
- ✓ Nachvollziehbarkeit der Zugriffe anhand der Benutzergruppen
- ✓ Protokollierung von Eingabe, Änderung und Löschung von Daten
- ✓ Authentizität (jederzeitige Datenzuordenbarkeit zu ihrem Ursprung)
- ✓ Übersicht der Applikationen, mit denen Daten eingegeben/geändert/gelöscht werden

Auftragskontrolle

- ✓ Auswahl weiterer (Sub-)Auftragsverarbeiter, z. B. Callcenter, nach Datensicherheitsgarantien
- ✓ Verpflichtung aller Auftragsverarbeiter gemäß Art. 28 Abs. 3 DSGVO
- ✓ Sorgfältige Auswahl von IT-, Wach-, Reinigungs-, Entsorgungs-, Transport- u. a. Dienstleistern
- ✓ Datenschutz-Audits beim Auftragsverarbeiter
- ✓ Sicherstellung der Rückgabe/ordnungsmäßigen Vernichtung aller Daten bei Vertragsbeendigung
- ✓ Beachtung der Voraussetzungen der DSGVO bei Auftragsdatenverarbeitung in Drittstaaten
- ✓ Risikobasierende Prüfungen von Auftragsdatenverarbeitungen in Drittstaaten

Verfügbarkeitskontrolle

- ✓ Datensicherungskonzept
- ✓ Führen von Backup-Verzeichnissen bzw. einer Backup-Verzeichnisstruktur
- ✓ Notfallplan/Recovery-Konzept
- ✓ Backup-Rechenzentrum
- ✓ Datenwiederherstellungstests
- ✓ Einsatz spezieller Monitoring-Programme zur Überwachung der Verfügbarkeit
- ✓ Unterbrechungsfreie Stromversorgung (USV)
- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöschgeräte
- ✓ Besonderer Brand-/Wassereintrittsschutz für Serverräume und Archive
- ✓ Temperatur-/Feuchtigkeitsüberwachung/Klimaanlage in Serverräumen und Archiven
- ✓ Schutzsteckdosenleisten in Serverräumen und Archiven
- ✓ Abgestimmte und umgesetzte Anforderungen für Datenverfügbarkeit und -verarbeitbarkeit
- ✓ Minimierung der Eintrittspunkte für Schadsoftware (Abschaltung verzichtbarer Dienste)

Trennungsprinzip

- ✓ Keine Mitbenutzung der Büroräume, Archive und Server durch Fremdfirmen

- ✓ Physisch getrennte Datenspeicherung auf gesonderten Systemen, Laufwerken und Datenträgern
- ✓ Logische Mandantentrennung
- ✓ Festlegung von Datenbankrechten (Zugriffsschranken für einzelne Ordner, Datensätze, Felder)
- ✓ Rollentrennung von Benutzern
- ✓ Berechtigungskonzept
- ✓ Verwaltung der Berechtigungen durch Systemadministrator
- ✓ Mittels Berechtigungskonzept getrennte Speicherung besonders sensibler Daten (z. B. Personalbereich)
- ✓ Trennung von Entwicklungs-, Test- und Produktivsystemen
- ✓ Trennung von Erfassungs- und Originaldaten (z. B. bei anonymisierten Daten)
- ✓ Informationelle Gewaltenteilung

Organisation

- ✓ Bestellung eines Datenschutzbeauftragten
- ✓ Verpflichtung der Mitarbeiter zur Wahrung des Datengeheimnisses
- ✓ Verpflichtung des Fremdpersonals zur Wahrung des Datengeheimnisses
- ✓ Datenschutz-Schulungen für Mitarbeiter
- ✓ Informationssicherheitsrichtlinien
- ✓ Regelung privater Nutzung betrieblicher Kommunikationstechnik
- ✓ Direkt-/Adressmarketing nach datenschutzrechtlichen Vorgaben
- ✓ Einsatz von Cloud Computing nach datenschutzrechtlichen Vorgaben
- ✓ Datenschutz-Richtlinie