Auftragsverarbeitungsvertrag

(AVV)

Vertrag über die Verarbeitung von personenbezogenen Daten im Auftrag

gemäß Art. 28 DSGVO

Zwischen

Longwall Security GmbH

Hauptstraße 27, 65529 Waldems, Deutschland

– nachfolgend bezeichnet als „Auftragsverarbeiter“ –

und

Kunden des Auftragsverarbeiters

– nachfolgend bezeichnet als „Auftraggeber“ –

Auftragsverarbeiter und Auftraggeber werden nachfolgend als „Vertragsparteien“ bezeichnet.

Alle Begrifflichkeiten verstehen sich geschlechtsneutral.

Präambel und Anwendungsbereich

Der Auftragsverarbeiter erbringt für den Auftraggeber IT-Dienstleistungen in den Bereichen IT-Sicherheit und IT-Infrastruktur. Das Leistungsspektrum umfasst insbesondere die Konzeption, Beratung, Optimierung, Konfiguration, den Betrieb und die Überwachung von IT-Lösungen sowie Incident Response, IT-forensische Untersuchungen bei Sicherheitsvorfällen und Schwachstellentests (Penetrationstests). Im Rahmen dieser Tätigkeiten verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Auftraggebers.

Dieser Auftragsverarbeitungsvertrag konkretisiert die Auftragsverarbeitung im Hinblick auf ihren Gegenstand und die sich aus dem Auftragsverarbeitungsverhältnis ergebenden Ansprüche und Pflichten zwischen den Vertragsparteien.

Der Auftragsverarbeitungsvertrag findet keine Anwendung, wenn die DSGVO auf die Verarbeitung von personenbezogenen Daten durch den Auftraggeber nicht anwendbar ist (zum Beispiel bei ausschließlich persönlichen oder familiären Tätigkeiten entsprechend Art. 2 Abs. 2 lit. c. DSGVO) und der Auftragsverarbeiter daher nicht als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO handelt.

§ 1 – Begrifflichkeiten und Definitionen

a. „Auftragsverarbeitung“ – Als Auftragsverarbeitung ist, im Einklang mit Art. 4 Nr. 8 DSGVO, die im Auftrag des Verantwortlichen durch den Auftragsverarbeiter entsprechend dem Gegenstand dieses Auftragsverarbeitungsvertrages erfolgende Verarbeitung personenbezogener Daten gem. Art. 4 Nr. 2 DSGVO zu verstehen.

b. „Hauptvertrag“ – Der Begriff des Hauptvertrages umfasst alle Arten laufender Geschäftsbeziehungen zwischen dem Auftraggeber und dem Auftragsverarbeiter, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten im Auftrag und auf Weisung des Auftraggebers verarbeitet. Der Hauptvertrag umfasst insbesondere den Dienstleistungsvertrag über IT-Sicherheits-, IT-Infrastruktur- und IT-Beratungsleistungen einschließlich Incident Response, IT-Forensik und Schwachstellentests sowie etwaige Rahmen- oder Einzelverträge.

c. „Verantwortlicher“ – Verantwortlicher ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO).

d. „Personenbezogene Daten“ – Personenbezogene Daten (nachfolgend auch kurz als „Daten“ bezeichnet) sind im Einklang mit Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen.

e. „Betroffene Personen“ – Als betroffene Personen werden entsprechend Art. 4 Nr. 1 DSGVO Personen bezeichnet, die mittels personenbezogener Daten zumindest identifizierbar sind.

f. „Dritte“ – Dritte sind entsprechend Art. 4 Nr. 10 DSGVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

g. „Unterauftragsverarbeitung“ – Wenn ein Auftragsverarbeiter nicht direkt vom Verantwortlichen beauftragt wurde, sondern von einem Auftragsverarbeiter des Verantwortlichen, liegt eine Unterauftragsverarbeitung vor. Die dem ersten Auftragsverarbeiter folgenden Auftragsverarbeiter werden als Unterauftragsverarbeiter bezeichnet.

h. „Elektronisches Format“ – Erklärungen gelten als im elektronischen Format entsprechend Art. 28 Abs. 9 DSGVO abgegeben, wenn die erklärende Person erkennbar ist und das elektronische Erklärungsformat sich zum Nachweis der Erklärung eignet (z. B. E-Mail, digitale Signierverfahren).

§ 2 – Gegenstand der Auftragsverarbeitung

a. Die Auftragsverarbeitung erfolgt im Rahmen des Hauptvertrages über die Erbringung von IT-Dienstleistungen, insbesondere die Konzeption, Beratung, Optimierung, Konfiguration, den Betrieb und die Überwachung von IT-Sicherheits- und IT-Infrastrukturlösungen sowie Incident Response, IT-forensische Untersuchungen bei Sicherheitsvorfällen und Schwachstellentests (Penetrationstests).

b. Detailangaben zum Gegenstand der im Auftrag erfolgenden Verarbeitung, die verarbeiteten personenbezogenen Daten, von der Verarbeitung betroffene Personen sowie Art, Umfang und Zweck der Verarbeitung, richten sich nach den Vorgaben des Anhangs „Gegenstand der Auftragsverarbeitung“.

§ 3 – Art der Auftragsverarbeitung

Soweit der Auftraggeber als Verantwortlicher der Auftragsverarbeitung handelt, ist er im Rahmen dieses Auftragsverarbeitungsvertrages für die Einhaltung der Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Rechtmäßigkeit der Beauftragung des Auftragsverarbeiters verantwortlich. Soweit der Auftraggeber selbst als Auftragsverarbeiter handelt, beauftragt er den Auftragsverarbeiter als Unterauftragsverarbeiter. Der Verantwortliche der Verarbeitung darf sich auf Grundlage dieses Auftragsverarbeitungsvertrages unmittelbar auf die dem Auftraggeber gegenüber dem Unterauftragsverarbeiter zustehenden Rechte berufen.

§ 4 – Weisungsbefugnis

a. Der Auftragsverarbeiter darf personenbezogene Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten und nur insoweit die Verarbeitung im Rahmen des Hauptvertrages erforderlich ist.

b. Die Weisungen werden anfänglich durch den Hauptvertrag oder diesen Auftragsverarbeitungsvertrag festgelegt und können vom Auftraggeber danach durch Weisungen in schriftlicher Form oder in einem elektronischen Format an den Auftragsverarbeiter geändert, ergänzt oder ersetzt werden.

c. Mündliche Weisungen können erfolgen, wenn sie aufgrund der Umstände (z. B. Eilbedürftigkeit) geboten sind und sind unverzüglich schriftlich oder in elektronischer Form zu bestätigen.

d. Ist der Auftragsverarbeiter aufgrund objektiver Umstände der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird der Auftragsverarbeiter den Auftraggeber unverzüglich darauf hinweisen und die Ansicht sachlich begründen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung bis zur ausdrücklichen Bestätigung der Weisung durch den Auftraggeber auszusetzen und offensichtlich rechtswidrige Weisungen abzulehnen.

e. Der Auftragsverarbeiter kann durch das Recht der Union oder der Mitgliedstaaten und behördliche sowie gerichtliche Maßnahmen zur Durchführung von Verarbeitungen verpflichtet werden. In einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber die rechtlichen Anforderungen der zwingenden gesetzlichen Verpflichtung vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht verbietet.

f. Der Auftragsverarbeiter hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

g. Der Auftragsverarbeiter benennt die zum Empfang von Weisungen berechtigten Ansprechpartner und ist verpflichtet, Änderungen der Ansprechpartner oder deren Kontaktinformationen unverzüglich mitzuteilen.

§ 5 – Wahrung des Berufsgeheimnisses

a. Die folgenden Verpflichtungen finden Anwendung, sofern die im Auftrag verarbeiteten Daten Berufsgeheimnisse im Sinne des § 203 StGB enthalten. Dies betrifft insbesondere Auftraggeber aus dem Gesundheitswesen, dem Rechts- und Steuerwesen sowie vergleichbare Berufsgeheimnisträger. Die Verpflichtungen gelten auch für die vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter.

b. Die Verpflichtungen gelten unabhängig von den zeitlichen Regelungen dieses Auftragsverarbeitungsvertrages auch nach Vertragsende zeitlich unbeschränkt.

c. Der Auftragsverarbeiter darf sich nur insoweit Kenntnis von Berufsgeheimnissen verschaffen, als dies für die Durchführung des Hauptvertrages sowie dieses Auftragsverarbeitungsvertrages und Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

d. Der Auftraggeber belehrt den Auftragsverarbeiter darüber, dass der Verstoß gegen die Vertraulichkeitsverpflichtungen durch Bruch der Verschwiegenheit oder die Verwertung fremder Geheimnisse gem. §§ 203 Abs. 1, Abs. 4 S. 1 StGB, § 204 StGB mit einer Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft werden kann. Die Strafandrohung erhöht sich auf eine Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bei Bereicherungsabsicht oder Schädigungsabsicht.

e. Sofern der Auftragsverarbeiter Dritte (z. B. Subunternehmer) beauftragt, die an der Auftragsverarbeitung mitwirken und Kenntnis von den Berufsgeheimnissen erlangen können, verpflichtet er die Dritten entsprechend zumindest in Textform zur Verschwiegenheit. Der Einsatz von Dritten bedarf der vorherigen Genehmigung des Auftraggebers. Der Auftraggeber erteilt mit Abschluss dieses Vertrages eine allgemeine Einwilligung zum Einsatz von Dritten, sofern diese gemäß lit. e auf Verschwiegenheit verpflichtet werden. Neue oder geänderte Dritte werden dem Auftraggeber vorab mitgeteilt; der Auftraggeber kann innerhalb von 14 Werktagen aus sachlichem Grund widersprechen.

§ 6 – Technische und organisatorische Maßnahmen

a. Der Auftragsverarbeiter wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als „TOMs“) zur angemessenen Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers treffen sowie deren Aufrechterhaltung, insbesondere durch regelmäßige, mindestens jährliche Evaluation, sicherstellen.

b. Die bei Vertragsschluss durch den Auftragsverarbeiter mitgeteilten TOMs definieren das vom Auftragsverarbeiter geschuldete Minimum des Sicherheitsniveaus. Die TOMs dürfen entsprechend dem technischen und rechtlichen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

c. Der Auftragsverarbeiter gewährleistet, dass es den mit der Verarbeitung befassten Mitarbeitern untersagt ist, die personenbezogenen Daten außerhalb der Weisung zu verarbeiten. Der Auftragsverarbeiter stellt ferner sicher, dass die zur Verarbeitung befugten Personen auf Vertraulichkeit und Verschwiegenheit verpflichtet worden sind.

d. Der Auftragsverarbeiter sorgt dafür, dass die bei ihm zur Verarbeitung eingesetzten Personen im Hinblick auf den Schutz personenbezogener Daten angemessen häufig an wiederkehrenden Schulungs- und Sensibilisierungsmaßnahmen teilnehmen.

e. Die Verarbeitung personenbezogener Daten außerhalb der Betriebsstätte des Auftragsverarbeiters (z. B. im Homeoffice oder bei Fernzugriff) ist zulässig, sofern die erforderlichen technischen und organisatorischen Maßnahmen ergriffen und dokumentiert werden.

f. Die Verarbeitung personenbezogener Daten auf Privatgeräten der Beschäftigten des Auftragsverarbeiters ist nicht zulässig.

g. Sofern durch gesetzliche Vorgaben vorgegeben, benennt der Auftragsverarbeiter einen den gesetzlichen Anforderungen entsprechenden Datenschutzbeauftragten und teilt dem Auftraggeber die Kontaktinformationen mit.

h. Die im Auftrag durchgeführten Verarbeitungsprozesse werden vom Auftragsverarbeiter in einem Verzeichnis von Verarbeitungstätigkeiten gesondert dokumentiert.

i. Die im Rahmen des Auftragsverarbeitungsvertrages überlassenen Daten sowie Datenträger verbleiben im Eigentum des Auftraggebers, sind durch den Auftragsverarbeiter sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers vernichtet werden.

j. Der Auftragsverarbeiter ist verpflichtet, eine nach diesem Auftragsverarbeitungsvertrag unverzüglich herbeizuführende Rückgabe bzw. Löschung der Daten auch bei Unterauftragsverarbeitern herbeizuführen.

k. Die Einrede eines Zurückbehaltungsrechts wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

l. Die bereits zum Abschluss dieses Auftragsverarbeitungsvertrages bestehenden technischen und organisatorischen Maßnahmen werden vom Auftragsverarbeiter im Anhang „Technische und organisatorische Maßnahmen“ aufgeführt.

§ 7 – Informations- und Mitwirkungspflichten des Auftragsverarbeiters

a. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Zustimmung durch den Auftraggeber oder im Fall zwingender gesetzlicher Pflichten erteilen. Wendet sich eine betroffene Person an den Auftragsverarbeiter und macht ihre Betroffenenrechte geltend, wird der Auftragsverarbeiter die betroffene Person an den Auftraggeber verweisen und den Antrag unverzüglich weiterleiten.

b. Der Auftragsverarbeiter hat den Auftraggeber unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung Fehler oder Unregelmäßigkeiten bei der Einhaltung von Datenschutzvorschriften feststellt.

c. Der Auftragsverarbeiter wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragsverarbeiter tätig wird und deren Tätigkeit die für den Auftraggeber verarbeiteten Daten betreffen kann.

d. Sollte die Sicherheit der personenbezogenen Daten des Auftraggebers durch Maßnahmen Dritter (z. B. Pfändung, Beschlagnahme, Insolvenzverfahren) gefährdet sein, wird der Auftragsverarbeiter die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen.

e. Der Auftragsverarbeiter stellt dem Auftraggeber Informationen zur Verfügung, die für die Erfüllung gesetzlicher Pflichten notwendig sind (insbesondere Anfragen Betroffener, Rechenschaftspflichten, Datenschutz-Folgenabschätzung) und unterstützt bei der Einhaltung der in Art. 32–36 DSGVO genannten Pflichten.

§ 8 – Maßnahmen bei Gefährdung oder Verletzung des Datenschutzes

a. Für den Fall, dass der Auftragsverarbeiter Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der personenbezogenen Daten im Sinne des Art. 4 Nr. 12 DSGVO verletzt sein könnte, hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten zu unterstützen.

b. Die Information über eine (mögliche) Verletzung des Schutzes personenbezogener Daten hat unverzüglich, grundsätzlich innerhalb von 48 Stunden ab dem Zeitpunkt zu erfolgen, zu dem der Auftragsverarbeiter gesicherte Kenntnis von der Verletzung erlangt hat. Eine gesicherte Kenntnis liegt vor, wenn der Auftragsverarbeiter nach einer angemessenen Erstbewertung des Vorfalls hinreichend sicher feststellen kann, dass personenbezogene Daten betroffen sind. Die reine Kenntnisnahme einer möglichen Anomalie oder eines Sicherheitsereignisses, das noch der Verifizierung bedarf, begründet für sich allein noch keine Meldepflicht.

c. Die Meldung des Auftragsverarbeiters muss entsprechend Art. 33 Abs. 3 DSGVO mindestens die folgenden Angaben beinhalten: Beschreibung der Art der Verletzung mit Angabe der betroffenen Kategorien von Daten und der ungefähren Zahl der betroffenen Personen; den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle; eine Beschreibung der wahrscheinlichen Folgen der Verletzung; eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung.

d. Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen.

§ 9 – Überprüfungen und Inspektionen

a. Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses Auftragsverarbeitungsvertrages jederzeit im erforderlichen Umfang zu kontrollieren und die erforderlichen Überprüfungen, einschließlich Inspektionen, durchzuführen.

b. Der Auftragsverarbeiter hat den Auftraggeber bei den Kontrollen und Inspektionen im erforderlichen Rahmen zu unterstützen.

c. Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten und sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage) anzumelden.

d. Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie den Schutz personenbezogener Daten Dritter Rücksicht nehmen.

e. Statt der Einsichtnahmen und der Vor-Ort-Kontrollen darf der Auftragsverarbeiter den Auftraggeber auf eine gleichwertige Kontrolle durch unabhängige Dritte, Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder geeignete Datenschutz- oder IT-Sicherheitszertifizierungen gem. Art. 42 DSGVO verweisen.

f. Der Auftraggeber übt sein Kontrollrecht grundsätzlich nicht häufiger als alle 12 Monate aus, es sei denn ein konkreter Anlass macht Kontrollen vor Ablauf dieses Zeitraums erforderlich.

§ 10 – Unterauftragsverhältnisse

a. Der Auftraggeber erklärt sich damit einverstanden, dass der Auftragsverarbeiter im Rahmen der Auftragsverarbeitung Unterauftragsverarbeiter einsetzen darf. Der Auftragsverarbeiter informiert den Auftraggeber mit einer angemessenen Vorfrist von regulär 14 Werktagen über neue Unterauftragsverarbeiter und gibt dem Auftraggeber die Möglichkeit, Einspruch gegen den Einsatz zu erheben. Erhebt der Auftraggeber keinen Einspruch innerhalb der Vorfrist, darf der Unterauftragsverarbeiter eingesetzt werden.

b. Nimmt der Auftragsverarbeiter die Dienste eines Unterauftragsverarbeiters in Anspruch, muss er dem Unterauftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegen, zu denen sich der Auftragsverarbeiter in diesem Auftragsverarbeitungsvertrag verpflichtet hat.

c. Der Auftragsverarbeiter wählt den Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung und der Zuverlässigkeit sorgfältig aus.

d. Der Auftragsverarbeiter hat die Einhaltung der Pflichten der Unterauftragsverarbeiter regelmäßig, spätestens alle 12 Monate, zu überprüfen und zu dokumentieren.

e. Die Rechte des Auftraggebers müssen auch gegenüber den Unterauftragsverarbeitern wirksam ausgeübt werden können.

f. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragsverarbeiter gegenüber dem Auftraggeber.

g. Verarbeitungen, die keinen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen und bei denen der Auftragsverarbeiter die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt (z. B. Reinigungs-, Telekommunikations- oder Transportleistungen), stellen keine Unterauftragsverarbeitung dar. Gleichwohl hat der Auftragsverarbeiter sicherzustellen, dass die Sicherheit der Daten hierbei nicht gefährdet wird.

h. Die bereits zum Abschluss dieses Auftragsverarbeitungsvertrages bestehenden Unterauftragsverhältnisse werden vom Auftragsverarbeiter im Anhang „Unterauftragsverarbeiter“ aufgeführt.

§ 11 – Räumlicher Bereich der Auftragsverarbeitung

a. Personenbezogene Daten werden im Rahmen der Auftragsverarbeitung grundsätzlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder der Schweiz verarbeitet.

b. Die Verarbeitung darf in Drittstaaten erfolgen, sofern die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, d. h. insbesondere auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission, wirksamer Standardschutzklauseln (Standard Contractual Clauses, SCC) oder anerkannter verbindlicher interner Datenschutzvorschriften.

c. Die Genehmigung von Unterauftragsverhältnissen durch den Auftraggeber erstreckt sich auch auf den räumlichen Bereich der Auftragsverarbeitung.

§ 12 – Pflichten des Auftraggebers

a. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen, Weisungen oder Verarbeitungsprozessen Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen feststellt.

b. Der Auftraggeber benennt die zum Empfang von Weisungen berechtigten Ansprechpartner und ist verpflichtet, Änderungen der Ansprechpartner oder deren Kontaktinformationen unverzüglich mitzuteilen.

c. Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch betroffene Personen, dritte Unternehmen, Stellen oder Behörden, verpflichtet sich der Auftraggeber, den Auftragsverarbeiter bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 13 – Haftung

Es gelten die gesetzlichen Haftungsregelungen, insbesondere Art. 82 DSGVO sowie im Falle des Einsatzes eines Unterauftragsverarbeiters Art. 28 Abs. 4 S. 2 DSGVO.

§ 14 – Laufzeit, Fortgeltung nach Vertragsende und Datenlöschung

a. Dieser Auftragsverarbeitungsvertrag wird mit dessen Unterzeichnung bzw. Abschluss in einem elektronischen Format wirksam.

b. Laufzeit und Ende dieses Auftragsverarbeitungsvertrages richten sich nach der Laufzeit und dem Ende des Hauptvertrages.

c. Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Pflichten dieses Auftragsverarbeitungsvertrages.

d. Nach Abschluss der Erbringung der Verarbeitungsleistungen wird der Auftragsverarbeiter alle personenbezogenen Daten und deren Kopien nach Wahl des Auftraggebers entweder vernichten oder zurückgeben, sofern nicht eine gesetzliche Verpflichtung zur Speicherung besteht. Die Vernichtung hat datenschutzgerecht zu erfolgen.

e. Abweichend von lit. d. dürfen forensische Beweismittel, Untersuchungsergebnisse und zugehörige Dokumentationen über das Vertragsende hinaus aufbewahrt werden, soweit dies für laufende oder absehbare Ermittlungs-, Straf- oder Zivilverfahren, für die Erfüllung gesetzlicher Aufbewahrungspflichten oder auf ausdrückliche Weisung des Auftraggebers erforderlich ist. Der Auftragsverarbeiter informiert den Auftraggeber über Art und voraussichtliche Dauer der weiteren Aufbewahrung. Die Daten unterliegen während der weiteren Aufbewahrung einer Zugriffsbeschränkung und dürfen ausschließlich für den genannten Zweck verarbeitet werden. Nach Wegfall des Aufbewahrungsgrundes erfolgt die unverzügliche datenschutzgerechte Löschung.

f. Die sich aus dem Auftragsverarbeitungsvertrag ergebenden Pflichten zum Schutz vertraulicher Informationen gelten auch nach Ende des Auftragsverarbeitungsvertrages fort.

g. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter zumindest drei Jahre auch über das Vertragsende hinaus aufzubewahren.

§ 15 – DORA-VO

Sofern der Auftraggeber finanzaufsichtsrechtlichen Anforderungen unterliegt, gelten die zusätzlichen Regelungen im Anhang „Zusatzvereinbarung betreffend einfache IKT-Dienstleistungen entsprechend DORA-VO“.

§ 16 – Schlussbestimmungen

a. Das anwendbare Recht bestimmt sich nach dem Hauptvertrag.

b. Der Gerichtsstandort bestimmt sich nach dem Hauptvertrag.

c. Der vorliegende Auftragsverarbeitungsvertrag stellt die vollständige, zwischen den Vertragsparteien getroffene Vereinbarung dar. Nebenabreden bestehen nicht.

d. Mit Zustandekommen dieses Auftragsverarbeitungsvertrages werden alle etwaigen früheren Verträge aufgehoben, die den gleichen Gegenstand der Auftragsverarbeitung betreffen.

e. Änderungen sowie Ergänzungen dieses Auftragsverarbeitungsvertrages müssen zumindest im elektronischen Format erfolgen.

f. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz den Regelungen des Hauptvertrages vor.

g. Sollten eine oder mehrere Bestimmungen dieses Auftragsverarbeitungsvertrages unwirksam sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt (Salvatorische Klausel).

Dieser Auftragsverarbeitungsvertrag ist Teil des Hauptvertrages und wird mit dessen Abschluss wirksam.

Anhang: Gegenstand der Auftragsverarbeitung

Zwecke der Auftragsverarbeitung

Personenbezogene Daten des Auftraggebers werden auf Grundlage dieses Auftragsverarbeitungsvertrages zu den folgenden Zwecken verarbeitet:

Konzeption, Beratung, Optimierung, Konfiguration, Betrieb und Überwachung der IT-Sicherheits- und IT-Infrastrukturlösungen des Auftraggebers. Dies umfasst insbesondere Endpoint-Protection- und EDR-Lösungen, Firewalls und Netzwerksicherheit, E-Mail-Security, SIEM- und Monitoring-Systeme, Server- und Netzwerkinfrastruktur, Virtualisierungs- und Cloud-Umgebungen sowie die zugehörige Remote-Administration, Patch- und Update-Management, Dokumentation und Reporting. Darüber hinaus umfasst die Verarbeitung:

– Incident Response: Reaktion auf und Bewältigung von IT-Sicherheitsvorfällen, einschließlich der Eindammung, Analyse und Beseitigung von Bedrohungen sowie der Wiederherstellung betroffener Systeme.

– IT-Forensik: Sicherung, Analyse und Auswertung digitaler Beweismittel bei Sicherheitsvorfällen, einschließlich der Untersuchung kompromittierter Systeme, Datenträger, Logdaten und Kommunikationsverläufe zur Aufklärung von Ursachen und Auswirkungen.

– Schwachstellentests (Penetrationstests): Durchführung autorisierter Sicherheitsüberprüfungen und simulierter Angriffe auf IT-Systeme, Netzwerke und Anwendungen des Auftraggebers zur Identifikation von Schwachstellen und zur Bewertung des Sicherheitsniveaus.

Arten und Kategorien von Daten

Zu den auf Grundlage dieses Auftragsverarbeitungsvertrages verarbeiteten Arten und Kategorien personenbezogener Daten gehören:

a. Protokoll- und Logdaten der IT-Sicherheits- und Infrastruktursysteme (z. B. Ereignisprotokolle, Bedrohungsmeldungen, Quarantäne-Einträge, Systemlogs, Auditlogs).

b. Netzwerk- und Verbindungsdaten (IP-Adressen, MAC-Adressen, Hostnamen, Portnummern, Verbindungszeitpunkte).

c. Benutzer- und Gerätedaten (Benutzernamen, Active-Directory-Kennungen, Gerätenamen, Betriebssysteminformationen).

d. E-Mail-Metadaten und -Inhalte (Absender, Empfänger, Betreffzeilen, Nachrichteninhalte – soweit im Rahmen der E-Mail-Security oder IT-forensischer Untersuchungen verarbeitet).

e. Ticket- und Vorgangsdaten (Beschreibungen von Sicherheitsvorfällen, Kommunikation im Ticketsystem).

f. Fernwartungsdaten (Sitzungsprotokolle, Zeitstempel von Remote-Zugriffen).

g. Forensische Daten: Im Rahmen von IT-forensischen Untersuchungen können zusätzlich folgende Datenkategorien verarbeitet werden: Datei- und Dateisysteminformationen (Dateinamen, Metadaten, gelöschte Dateien), Browserverläufe und Applikationsdaten, forensische Abbilder (Images) von Datenträgern, Arbeitsspeicher-Dumps, Kommunikationsverläufe (E-Mail-, Chat- und Messaging-Inhalte) sowie Benutzeraktivitätsprotokolle. Art und Umfang richten sich nach dem konkreten Untersuchungsauftrag des Auftraggebers.

h. Schwachstellendaten: Im Rahmen von Penetrationstests und Schwachstellenanalyse verarbeitete Daten, insbesondere Scan-Ergebnisse, identifizierte Schwachstellen, Diensterkennungsdaten (offene Ports, Softwareversionen, Bannerdaten), Zugangsdaten (soweit im Rahmen des Tests autorisiert bereitgestellt) und Exploit-Nachweise.

i. Bestandsdaten der Ansprechpartner des Auftraggebers (Name, Funktion, Kontaktdaten).

Kategorien der betroffenen Personen

a. Mitarbeiter, Auszubildende und freie Mitarbeiter des Auftraggebers.

b. IT-Administratoren und Ansprechpartner des Auftraggebers.

c. Dritte, deren personenbezogene Daten in den Logdaten oder Sicherheitsmeldungen enthalten sind (z. B. externe Kommunikationspartner, Angreifer-IP-Adressen).

d. Patienten, Mandanten oder Kunden des Auftraggebers, soweit deren Daten in den verarbeiteten Protokolldaten oder forensischen Untersuchungsdaten enthalten sind.

e. Personen, deren personenbezogene Daten im Rahmen von IT-forensischen Untersuchungen auf kompromittierten Systemen, Datenträgern oder in Kommunikationsverläufen vorgefunden werden (z. B. Absender und Empfänger von E-Mails, Chat-Teilnehmer, Nutzer kompromittierter Accounts).

f. Personen, deren Daten im Rahmen von Schwachstellentests auf den geprüften Systemen angetroffen werden (z. B. in Datenbanken, Konfigurationsdateien oder Anwendungen gespeicherte personenbezogene Daten).

Quellen der verarbeiteten Daten

a. Automatisierte Erhebung durch IT-Sicherheits- und Infrastruktursysteme des Auftraggebers (z. B. Endpoint Protection, Firewalls, Netzwerkkomponenten, Server, Virtualisierungsplattformen).

b. Eingaben und Angaben des Auftraggebers im Rahmen von Supportanfragen und Konfigurationsaufträgen.

c. Erhebung im Rahmen der Remote-Administration und -Überwachung (RMM).

d. Forensische Sicherung: Erfassung von Daten aus kompromittierten Systemen, Datenträgern, Netzwerkmitschnitten und Speicherabbildern im Rahmen von IT-forensischen Untersuchungen auf Weisung des Auftraggebers.

e. Schwachstellenscans und Penetrationstests: Automatisierte und manuelle Erhebung von System- und Netzwerkdaten im Rahmen autorisierter Sicherheitsüberprüfungen auf Weisung des Auftraggebers.

f. Übermittlung durch oder im Auftrag des Auftraggebers.

Anhang: Technische und organisatorische Maßnahmen (TOMs)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden insbesondere die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste berücksichtigt.

Organisatorische Maßnahmen

a. Der Auftragsverarbeiter hat ein angemessenes Datenschutzmanagementsystem implementiert.

b. Es sind interne Sicherheitsrichtlinien definiert, die unternehmensintern als verbindliche Regeln kommuniziert werden.

c. Es werden regelmäßig System- und Sicherheitstests (z. B. Penetrationstests) durchgeführt.

d. Die Entwicklung des Stands der Technik sowie Bedrohungen und Sicherheitsmaßnahmen werden fortlaufend beobachtet.

e. Es besteht ein Konzept zur Wahrung der Betroffenenrechte sowie ein Konzept für die Reaktion auf Datenschutzverletzungen.

f. Sicherheitsvorkommnisse werden konsequent dokumentiert (Security Reporting).

g. Eingesetzte Software und Hardware wird stets auf dem aktuell verfügbaren Stand gehalten.

h. Es liegt ein den Datenschutzanforderungen entsprechendes Lösch- und Entsorgungskonzept vor.

Datenschutz auf Mitarbeiterebene

a. Mitarbeiter werden auf Vertraulichkeit und Verschwiegenheit verpflichtet.

b. Mitarbeiter werden im Hinblick auf den Datenschutz entsprechend ihren Funktionen regelmäßig geschult und sensibilisiert.

c. Ausgegebene Schlüssel, Zugangskarten oder Codes werden nach Ausscheiden eingezogen bzw. entzogen.

d. Es gilt eine Clean-Desk-Policy.

Zutrittskontrolle

a. Personenkontrolle beim Zutritt zu Räumlichkeiten mit Datenverarbeitungsanlagen.

b. Protokollierung der Ausgabe und Rückgabe von Schlüsseln und Zugangskarten.

c. Mitarbeiter werden verpflichtet, Geräte zu sperren, wenn sie den Arbeitsplatz verlassen.

d. Sichere Aufbewahrung von Unterlagen und Datenträgern.

Zugangskontrolle

a. Passwortkonzept mit Mindestlänge und Komplexitätsanforderungen entsprechend dem Stand der Technik.

b. Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.

c. Passwörter werden grundsätzlich nicht im Klartext gespeichert und nur gehashed oder verschlüsselt übertragen.

d. Zugangsdaten werden bei Ausscheiden aus dem Unternehmen gelöscht oder deaktiviert.

e. Einsatz von Angriffserkennungssystemen (Intrusion-Detection-Systemen) und Angriffsvermeidungssystemen (Intrusion-Protection-Systemen).

f. Einsatz aktueller Anti-Viren-Software sowie Hardware- und Software-Firewalls.

g. Mehrstufige Authentifizierung (Multi-Faktor-Authentifizierung) für den Zugang zu administrativen Konsolen und Kundensystemen.

Zugriffs- und Eingabekontrolle

a. Rechte- und Rollenkonzept (Berechtigungskonzept) nach dem Prinzip der minimalen Berechtigung.

b. Regelmäßige Evaluation des Berechtigungskonzepts.

c. Protokollierung von Anmeldungen und administrativen Tätigkeiten in den Datenverarbeitungssystemen.

d. Nachvollziehbarkeit, welche Beschäftigten auf welche Daten wann Zugriff hatten.

Weitergabekontrolle

a. Verschlüsselte Verbindung bei Fernzugriff auf Kundensysteme (VPN, TLS).

b. Transportverschlüsselung für E-Mails.

c. TLS-Verschlüsselung für sämtliche webbasierte Verwaltungsoberflächen und Konsolen.

Auftragskontrolle, Zweckbindung und Trennungskontrolle

a. Gesonderte Dokumentation der Verarbeitungsprozesse je Auftraggeber.

b. Sorgfältige Auswahl von Unterauftragsverarbeitern und sonstigen Dienstleistern.

c. Logische Trennung der Kundendaten (mandantenfähige Systeme, separate Tenant-Umgebungen in den eingesetzten Verwaltungs- und RMM-Plattformen).

d. Strikte Trennung von Produktiv- und Testsystemen.

Sicherung der Integrität und Verfügbarkeit

a. Einsatz ausfallsicherer, redundanter Serversysteme.

b. Permanentes Monitoring der Verfügbarkeit aller Verwaltungssysteme.

c. Regelmäßiges Patch-Management und dokumentierte Aktualisierungszyklen.

d. Zuverlässiges und kontrolliertes Backup- und Wiederherstellungskonzept.

e. Regelmäßige Wiederherstellungstests zur Überprüfung der Datenintegrität der Backups.

Besondere Maßnahmen für Incident Response, IT-Forensik und Schwachstellentests

a. Beweismittelsicherung (Chain of Custody): Bei IT-forensischen Untersuchungen wird eine lückenlose Dokumentation der Beweismittelkette geführt. Jeder Zugriff auf forensische Daten, jede Sicherung und jede Weitergabe wird mit Zeitstempel, handelnder Person und Zweck protokolliert.

b. Verschlüsselte Speicherung forensischer Daten: Forensische Abbilder (Images), Speicherdumps und sonstige Untersuchungsdaten werden ausschließlich verschlüsselt gespeichert und übertragen. Der Zugriff ist auf die an der Untersuchung beteiligten Personen beschränkt.

c. Vier-Augen-Prinzip: Der Zugriff auf forensische Beweismittel und Schwachstellentest-Ergebnisse, die besonders sensible personenbezogene Daten enthalten (z. B. Gesundheitsdaten, Kommunikationsinhalte), erfolgt grundsätzlich unter Anwendung des Vier-Augen-Prinzips.

d. Dedizierte forensische Arbeitsumgebung: Forensische Untersuchungen werden in einer vom Regelbetrieb getrennten, dedizierten Umgebung durchgeführt, um eine Kontamination oder unbeabsichtigte Vermischung mit anderen Kundendaten zu verhindern.

e. Löschkonzept für forensische Daten: Nach Abschluss einer forensischen Untersuchung und Übergabe der Ergebnisse an den Auftraggeber werden sämtliche forensischen Daten, Arbeitskopien und Zwischenergebnisse datenschutzgerecht gelöscht, sofern keine gesetzliche Aufbewahrungspflicht oder ein laufendes Ermittlungs- oder Gerichtsverfahren eine weitere Aufbewahrung erfordert. Die Löschung wird dokumentiert und dem Auftraggeber auf Anfrage bestätigt.

f. Autorisierung von Schwachstellentests: Penetrationstests und Schwachstellenscans werden ausschließlich auf Grundlage einer dokumentierten, schriftlichen Autorisierung des Auftraggebers durchgeführt, die den Umfang, die betroffenen Systeme und den Zeitraum der Tests festlegt.

g. Sichere Ergebnisübermittlung: Ergebnisse forensischer Untersuchungen und Schwachstellentests werden ausschließlich über verschlüsselte Kanäle an den Auftraggeber übermittelt und nicht unverschlüsselt per E-Mail versendet.

Anhang: Unterauftragsverarbeiter

Der Auftragsverarbeiter setzt die folgenden Unterauftragsverarbeiter im Rahmen der Verarbeitung von Daten für den Auftraggeber ein:

Sophos Technology GmbH	
Kategorie	SaaS-/Tool-Anbieter (Endpoint Security & Firewall-Management)
Anschrift	Gustav-Stresemann-Ring 1, 65189 Wiesbaden, Deutschland
Website	www.sophos.com
Leistungsgegenstand	Sophos Central Partner-Portal: Cloud-basierte Verwaltung und Überwachung von Endpoint-Protection-, EDR- und Firewall-Lösungen des Auftraggebers. Verarbeitete Daten: Logdaten, Bedrohungsmeldungen, Quarantäne-Einträge, Benutzernamen, Geräteinformationen.
Standort der Verarbeitung	EU/EWR, UK
Drittlandtransfer-Grundlage	EU-UK Angemessenheitsbeschluss
Auftragsverarbeitungsvertrag	https://www.sophos.com/en-us/legal/data-processing-agreement
Datenschutzerklärung	https://www.sophos.com/en-us/legal/sophos-group-privacy-notice
Letzte Prüfung	13.04.2026

Atera Networks Ltd.	
Kategorie	SaaS-/Tool-Anbieter (Remote Monitoring & Management)
Anschrift	Königsborner Str. 35B, 59427 Unna, Deutschland (EU-Niederlassung); Hauptsitz: 244 Madison Avenue, New York, NY 10016, USA
Website	www.atera.com
Leistungsgegenstand	Remote Monitoring & Management (RMM): Fernwartung, Überwachung, Patch-Management, Inventarisierung und Ticketing für Kundensysteme. Verarbeitete Daten: Gerätedaten, Benutzernamen, IP-Adressen, Monitoring-Daten, Sitzungsprotokolle.
Standort der Verarbeitung	EU/EWR, Israel, USA
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	Auf Anfrage bei: success@atera.com
Datenschutzerklärung	https://www.atera.com/privacy/
Letzte Prüfung	13.04.2026

TeamViewer Germany GmbH	
Kategorie	SaaS-/Tool-Anbieter (Remote-Zugriff)
Anschrift	Bahnhofsplatz 2, 73033 Göppingen, Deutschland
Website	www.teamviewer.com
Leistungsgegenstand	Remote-Zugriff auf Kundensysteme zu Zwecken der Administration, Fehlerbehebung und Konfiguration. Verarbeitete Daten: Sitzungsdaten, TeamViewer-IDs, IP-Adressen, Verbindungszeitpunkte, übertragene Inhalte (Bildschirm, Dateien, Chat).
Standort der Verarbeitung	EU/EWR (Hauptstandort Deutschland); Sub-Prozessoren überwiegend im EWR
Drittlandtransfer-Grundlage	Standardvertragsklauseln (SCC) für Ausnahmen außerhalb des EWR
Auftragsverarbeitungsvertrag	https://www.teamviewer.com/en/legal/eula/ (DPA im EULA integriert)
Datenschutzerklärung	https://www.teamviewer.com/en/legal/privacy-and-cookies/
Letzte Prüfung	13.04.2026

Microsoft Ireland Operations Limited	
Kategorie	SaaS-/Tool-Anbieter (Productivity & Collaboration)
Anschrift	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Website	www.microsoft.com
Leistungsgegenstand	Microsoft 365 (Outlook, Teams, OneDrive, SharePoint): Cloud-basierte E-Mail-Kommunikation, Dokumentenverwaltung, Videokonferenzen, Chat und Collaboration. Verarbeitete Daten: E-Mails, Dateien, Chat-Nachrichten, Kalendereinträge, Meeting-Daten, Kontaktdaten.
Standort der Verarbeitung	EU/EWR
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
Datenschutzerklärung	https://privacy.microsoft.com/de-de/privacystatement
Letzte Prüfung	13.04.2026

Zoom Video Communications Inc.	
Kategorie	SaaS-/Tool-Anbieter (Videokonferenzen)
Anschrift	55 Almaden Boulevard, 6th Floor, San Jose, CA 95113, USA
Website	www.zoom.us
Leistungsgegenstand	Videokonferenzen: Durchführung von Online-Meetings mit Kunden und internen Teilnehmern. Verarbeitete Daten: Teilnehmernamen, E-Mail-Adressen, IP-Adressen, Meeting-Metadaten, ggf. Aufzeichnungen.
Standort der Verarbeitung	EU/EWR, USA
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://explore.zoom.us/de/data-processing-addendum/
Datenschutzerklärung	https://explore.zoom.us/de/privacy/
Letzte Prüfung	13.04.2026

AgileBits Inc. (1Password)	
Kategorie	SaaS-/Tool-Anbieter (Passwort-Management)
Anschrift	4711 Yonge Street, 10th Floor, Toronto, Ontario, M2N 6K8, Kanada
Website	www.1password.com
Leistungsgegenstand	Passwort-Management: Zentrale Verwaltung und sichere Speicherung von Zugangsdaten für Kundensysteme (Verwaltungskonsolen, Firewalls, RMM, Remote-Zugriff, Infrastrukturkomponenten). Verarbeitete Daten: Verschlüsselte Vault-Daten, Benutzernamen, E-Mail-Adressen.
Standort der Verarbeitung	Kanada, USA, EU/EWR
Drittlandtransfer-Grundlage	EU-Kanada Angemessenheitsbeschluss; Standardvertragsklauseln (SCC) für US-Verarbeitung
Auftragsverarbeitungsvertrag	https://1password.com/legal/data-processing-addendum
Datenschutzerklärung	https://1password.com/legal/privacy/
Letzte Prüfung	13.04.2026

Slack Technologies LLC (Salesforce Inc.)	
Kategorie	SaaS-/Tool-Anbieter (Interne Kommunikation)
Anschrift	Salesforce Tower, 415 Mission Street, San Francisco, CA 94105, USA
Website	www.slack.com
Leistungsgegenstand	Interne Kommunikation und Collaboration: Team-Messaging, Datei-Austausch und Koordination. Verarbeitete Daten: Nachrichten, Benutzernamen, E-Mail-Adressen und geteilte Dateien, soweit Kundendaten in der Kommunikation enthalten sind.
Standort der Verarbeitung	EU/EWR, USA
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://slack.com/trust/compliance/gdpr
Datenschutzerklärung	https://slack.com/intl/de-de/trust/privacy/privacy-policy
Letzte Prüfung	13.04.2026

Rapid7 Germany GmbH	
Kategorie	SaaS-/Tool-Anbieter (Schwachstellenmanagement & SIEM)
Anschrift	Am Söldnermoos 17, 85399 Hallbergmoos, Deutschland; Amtsgericht München HRB 212466
Website	www.rapid7.com/de
Leistungsgegenstand	IT-Sicherheitsplattform: Schwachstellenmanagement (InsightVM), SIEM/XDR (InsightIDR), Cloud-Sicherheit und Incident-Response-Services für Kundensysteme. Verarbeitete Daten: Netzwerk-Scandaten, Logdaten, Schwachstelleninformationen, IP-Adressen, Hostnamen, Benutzerkennungen, Sicherheitsereignisse.
Standort der Verarbeitung	EU/EWR, USA (AWS-Infrastruktur)
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://www.rapid7.com/legal/dpa/
Datenschutzerklärung	https://www.rapid7.com/privacy-policy/
Letzte Prüfung	13.04.2026

RelationFlow Ltd. (Voicely)	
Kategorie	SaaS-/Tool-Anbieter (KI-gestützte Spracherkennung)
Anschrift	Anthypolochagou Georgiou M. Savva 26, Office 1-2, 8201 Paphos, Zypern
Website	www.voicely.de
Leistungsgegenstand	KI-gestützte Spracherkennung und Diktiersoftware (Speech-to-Text): Umwandlung von Spracheingaben in Text für interne Dokumentation und Kommunikation. Im Privacy Mode erfolgt die Verarbeitung vollständig lokal auf dem Endgerät. Verarbeitete Daten: Audiodaten (Spracheingaben) und daraus generierte Textdaten.
Standort der Verarbeitung	EU/EWR (Server: Frankfurt, Deutschland)
Drittlandtransfer-Grundlage	Entfällt – Verarbeitung ausschließlich innerhalb der EU/EWR
Auftragsverarbeitungsvertrag	Auf Anfrage bei: info@relationflow.io
Datenschutzerklärung	https://www.voicely.de/datenschutz
Letzte Prüfung	13.04.2026

OpenAI, LLC (ChatGPT Business / Team)	
Kategorie	SaaS-/Tool-Anbieter (KI-Sprachmodell-Dienste)
Anschrift	OpenAI, LLC, 3180 18th Street, San Francisco, CA 94110, USA; für EU-Kunden: OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland
Website	www.openai.com
Leistungsgegenstand	KI-basierte Sprachmodell-Dienste (ChatGPT Business/Team): Unterstützung bei interner Dokumentation, Analyse, Recherche und Textverarbeitung. Verarbeitete Daten: Texteingaben (Prompts), die personenbezogene Daten enthalten können, generierte Antworten sowie hochgeladene Dateien. Eingaben werden im Business/Team-Tarif nicht zur Modellverbesserung verwendet.
Standort der Verarbeitung	USA; EU-Datenhaltung optional bei Enterprise-Tarif
Drittlandtransfer-Grundlage	EU-US Data Privacy Framework; Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://openai.com/policies/data-processing-addendum
Datenschutzerklärung	https://openai.com/policies/privacy-policy
Letzte Prüfung	13.04.2026

Anthropic PBC (Claude Team)	
Kategorie	SaaS-/Tool-Anbieter (KI-Sprachmodell-Dienste)
Anschrift	548 Market Street, PMB 90375, San Francisco, CA 94104, USA
Website	www.anthropic.com
Leistungsgegenstand	KI-basierte Sprachmodell-Dienste (Claude Team): Unterstützung bei interner Dokumentation, Analyse, Recherche und Textverarbeitung. Verarbeitete Daten: Texteingaben (Prompts), die personenbezogene Daten enthalten können, generierte Antworten sowie hochgeladene Dateien.
Standort der Verarbeitung	USA
Drittlandtransfer-Grundlage	Standardvertragsklauseln (SCC)
Auftragsverarbeitungsvertrag	https://www.anthropic.com/legal/commercial-terms
Datenschutzerklärung	https://www.anthropic.com/legal/privacy
Letzte Prüfung	13.04.2026

LW IT Secure GmbH	
Kategorie	Operativer IT-Dienstleister (Unterauftragsverarbeiter für IT-Sicherheitsdienstleistungen)
Anschrift	Im Hopfenstück 2, 65510 Idstein, Deutschland
Website	www.lwsecure.de
Leistungsgegenstand	Erbringung operativer IT-Sicherheitsdienstleistungen im Namen und auf Weisung des Auftragsverarbeiters gegenüber dessen Kunden: Managed SOC/Monitoring (24/7-Überwachung, Threat Detection & Response, Incident Handling), Incident Response und IT-Forensik (forensische Sicherung und Analyse kompromittierter Systeme), Vor-Ort-Einsätze sowie IT-Consulting. Direkter Zugriff auf Kundensysteme; Verarbeitung sämtlicher im AVV genannter Datenkategorien einschließlich forensischer Daten und Schwachstellendaten, soweit zur Erfüllung der beauftragten Leistung erforderlich.
Standort der Verarbeitung	Deutschland (EU/EWR)
Drittlandtransfer-Grundlage	Entfällt – Verarbeitung ausschließlich innerhalb der EU/EWR
Auftragsverarbeitungsvertrag	Separater Auftragsverarbeitungsvertrag zwischen Longwall Security GmbH und LW IT Secure GmbH
Datenschutzerklärung	Auf Anfrage bei: info@lwsecure.de
Letzte Prüfung	13.04.2026

Anhang: Zusatzvereinbarung betreffend einfache IKT-Dienstleistungen entsprechend DORA-VO

Der Auftragnehmer erkennt an, dass der Auftraggeber als Finanzunternehmen spezielle aufsichtsrechtliche Anforderungen erfüllen muss, insbesondere die Verordnung (EU) 2022/2554 vom 14. Dezember 2022 zur digitalen operativen Resilienz im Finanzsektor (DORA-VO). Diese Regelungen haben Vorrang vor den übrigen vertraglichen Vereinbarungen der Parteien.

1. Gegenstand, Art und Qualität der IKT-Dienstleistung

1.1. Der Auftragnehmer stellt dem Auftraggeber die im Auftragsverarbeitungsvertrag spezifizierten IKT-Dienstleistungen zur Verfügung. Dies umfasst die Konzeption, Beratung, Optimierung, Konfiguration, den Betrieb und die Überwachung von IT-Sicherheits- und IT-Infrastrukturlösungen sowie Incident Response, IT-forensische Untersuchungen und Schwachstellentests.

1.2. Der Auftragnehmer erbringt ausschließlich einfache IKT-Dienstleistungen. Diese sind definiert als Dienstleistungen, die nicht zur Unterstützung kritischer oder wichtiger Funktionen gemäß Artikel 3 Nummer 22 der DORA-VO genutzt werden.

1.3. Der Auftragnehmer verpflichtet sich, die Dienstleistungen in der vertraglich vereinbarten Qualität zu erbringen und dabei alle für den Auftraggeber geltenden gesetzlichen und aufsichtsrechtlichen Vorgaben zu beachten.

1.4. Der Auftragnehmer sichert zu, dass er alle notwendigen Genehmigungen und Registrierungen zur Erfüllung seiner Verpflichtungen besitzt.

2. Standorte der Leistungserbringung

Die Bereitstellung der vertraglich vereinbarten IKT-Dienstleistungen erfolgt an den im Anhang „Unterauftragsverarbeiter“ genannten Standorten. Änderungen dieser Standorte müssen dem Auftraggeber mit einer Frist von mindestens 8 Wochen im Voraus in Textform mitgeteilt werden.

3. Einhaltung von Gesetzen, Standards und Datenschutz

3.1. Der Auftragnehmer verpflichtet sich, bei der Erbringung der Dienstleistungen alle für den Auftraggeber geltenden gesetzlichen Standards einzuhalten, insbesondere in Bezug auf Datenschutz und Bankgeheimnis.

3.2. Der Auftragnehmer verpflichtet sich, dem Auftraggeber alle notwendigen Informationen offenzulegen, die für die Durchführung einer erforderlichen Risikoanalyse oder Aufsichtsprüfung benötigt werden.

Unterschriften

Ort, Datum

Auftragsverarbeiter – Longwall Security GmbH

Name, Funktion, Unterschrift

Auftraggeber

Name, Funktion, Unterschrift