Vertrag zur Auftragsverarbeitung personenbezogener Daten

Stand: 23. Februar 2026

zwischen

_____

_____

_____

_____

mit der **Kundennummer**

_____

im folgenden **Auftraggeber** genannt

und

vio:networks GmbH
Oberschwaigstraße 45
92237 Sulzbach Rosenberg
Telefon +49 30 2084701 0
E-Mail team@vionetworks.de

im folgenden **Auftragnehmer** genannt

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in 3. genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

1. Begriffsbestimmungen

1) Verantwortlicher ist gem. Art. 4 Abs. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DS-GVO, biometrischen Daten gem. Art. 4 Abs. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5) Verarbeitung ist gem. Art. 4 Abs. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

2. Angabe der zuständigen Datenschutz-Aufsichtsbehörde

1) Zuständige Aufsichtsbehörde für den Auftragnehmer ist der Bayerische Landesbeauftragte für den Datenschutz Herr Dr. Thomas Petri.

2) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

3. Vertragsgegenstand

1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Telekommunikation/Cloud-Telefonanlage auf Grundlage des vom Auftraggeber gestellten Auftrages („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und der dazugehörigen Leistungsbeschreibung). Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der 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.

4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

4. Weisungsrecht

1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; 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 Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. 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 Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, 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 Weisung ablehnen.

5. Art der verarbeiteten Daten, Kreis der Betroffenen

1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.

2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.

6. Schutzmaßnahmen des Auftragnehmers

1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind 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. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der:

    1) Zutrittskontrolle
    2) Zugangskontrolle
    3) Zugriffskontrolle
    4) Weitergabekontrolle
    5) Eingabekontrolle
    6) Auftragskontrolle
    7) Verfügbarkeitskontrolle
    8) Trennungskontrolle
    9) Datenschutz-Managementsystem

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

3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/Ansprechpartner für den Datenschutz bestellt: Frau Severine Petersen. Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Beschäftigte/Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

7. 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 Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

    1) 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;

    2) eine Beschreibung der von dem 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, informiert hierüber den Auftraggeber und ersucht 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) 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 DS-GVO liegen.

5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach 6. Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

7) 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 DS-GVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

8. Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

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) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach 6. Abs. 4 auf Verlangen nach.

9. Einsatz von Subunternehmern

1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Die weitere Auslagerung auf Unterauftragnehmer sowie der Wechsel von bestehenden Unterauftragnehmern ist zulässig, soweit (a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und (b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und (c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. 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 direkt 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.

2) 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.

10. Anfragen und Rechte Betroffener

1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DS-GVO.

2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

11. Haftung

1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

12. Außerordentliches Kündigungsrecht

1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

13. 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 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. Zu entsorgende Datenträger sind nach DIN 66399-1 bzw. DIN 66399-2 zu vernichten, hierbei werden die Daten auf der Sicherheitsstufe 2 bis Sicherheitsstufe 4 vernichtet, nach dem Grad der Vertraulichkeit.

2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

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.

14. 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. 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) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Sulzbach-Rosenberg.

Anlagen

1) Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

2) Beschreibung der Betroffenen/Betroffenengruppen

3) Technische und organisatorische Maßnahmen des Auftragnehmers

4) Genehmigte Subunternehmer

1) Weisungsberechtigte Personen

Unterschriften

_____	_____
Ort und Datum	Ort und Datum
_____	_____
Unterschrift vio:networks GmbH / Auftragnehmer	Unterschrift Auftraggeber
_____	_____
Name in Druckbuchstaben	Name in Druckbuchstaben
_____	_____
Funktion	Funktion

Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

- Nachname/Vorname
- Anschrift
- Kontaktdaten (Telefon, Mobilfunk, Fax, E-Mail, Website)
- Verkehrsdaten (z.B. Telefonverbindung)
- Vertragsstammdaten (z.B. Kundennummer, Firmenkennung, Ansprechpartner, Auftragsunterlagen, Bankverbindung, Unterschrift, ehemalige Anbieter, Rufnummern)
- Abrechnungsdaten (z. B. Anzahl der gebuchten Nebenstellen/Benutzer, Bestellungen, Telefonverbindung)
- Kundenhistorie (z.B. Korrespondenzen, Gesprächsnotizen, Bestellhistorie)

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

- Beschäftigte/Mitarbeiter
- Kunden
- Lieferanten

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

1) Zutrittskontrolle

   Die Maßnahmen zur Zutrittssicherheit sind abhängig vom Einsatzzweck der Räumlichkeiten und dem Schutzbedarf der Systeme, die sich in ihnen befinden.

   Sensible Datenverarbeitungsanlagen befinden sich immer in entsprechend geschützten Räumlichkeiten wie z.B. dem Rechenzentrum des Auftragnehmers. Das Betriebsgelände des Rechenzentrums ist umzäunt und wird mit einer Videoanlage, z.T. Bewegungsmeldern und einer Einbruchmeldeanlage überwacht. Es existieren technische und organisatorische Maßnahmen zur Beschränkung des Zutritts zu geschützten Bereichen für interne und externe Personen. Ebenso existiert ein Rechtssystem für den Zutritt zu besonders schätzenswerten Bereichen.

   Der Zugang zu den Büroräumlichkeiten des Auftragnehmers ist auf die Beschäftigten bzw. Mitarbeiter beschränkt. Gäste werden in den Räumlichkeiten stets begleitet.

   Der Auftragnehmer hat die Eignung des Arbeitsplatzes für Beschäftigte bzw. Mitarbeiter im Home Office kontrolliert und gewährleistet den Datenschutz in den von Beschäftigten bzw. Mitarbeitern genutzten Räumen. Der Auftragnehmer hat sich hierzu sowohl die Berechtigung zum Zutritt des zur Arbeit genutzten Raumes der Beschäftigten als auch eventueller weiterer Personen des Haushalts eingeholt.

2) Zugangskontrolle

   Zum Zugang zu Systemen muss sich der Nutzer grundsätzlich mittels eines Verfahrens auf dem aktuellen Stand der Technik authentisieren. Bei Systemen mit besonders hohem Schutzbedarf sind zusätzliche Verfahren etabliert.

   Die Zugangsberechtigung wird beantragt und von dem verantwortlichen Vorgesetzten genehmigt. Der Zugang zu Applikationen und zu Informationen erfolgt auf Basis von Rollen und dem konkreten geschäftlichen Bedarf der Benutzer (Prinzip der minimalen Berechtigung/Need To Know Prinzip). Passwortlänge, Komplexität und Gültigkeit werden verbindlich vorgegeben und die Vorgaben werden kontinuierlich an aktuelle Anforderungen angepasst. Fehlerhafte Anmeldungen werden soweit sinnvoll und technisch machbar protokolliert und bei Bedarf ausgewertet.

Der Zugang zu datenschutzrelevanten Kundendaten erfolgt nur mittels einer gesicherten VPN, für diese sichert der Auftragnehmer die höchsten Sicherheitsstandards zu.

Die Hardware aller Beschäftigten bzw. Mitarbeiter des Auftragnehmers ist passwortgeschützt, dies trifft vor allem auch auf die im Home Office genutzten Geräte zu, welche von dem Auftragnehmer zur Verfügung gestellt werden.

Beim Verlassen des Arbeitsplatzes wird die genutzte Hardware mittels Bildschirmsperre vor der Nutzung durch unbefugte Dritte geschützt.

3) Zugriffskontrolle

Die Zugriffsberechtigung muss beantragt und von dem verantwortlichen Vorgesetzten genehmigt werden.

Der Berechtigungsprozess beinhaltet den Entzug von Zugriffsberechtigungen im Falle eines Wechsels in der Verantwortung oder bei Ausscheiden eines Mitarbeiters aus dem Unternehmen.

Eine Kontrolle der Berechtigungsvergaben erfolgt anlassbezogen und regelmäßig im Rahmen interner Audits.

4) Weitergabekontrolle

Die Datenübertragung zwischen vertrauenswürdigen Netzen über öffentliche/nicht vertrauenswürdige Netze erfolgt verschlüsselt.

Eine Weitergabe der Daten zur Weiterverarbeitung an Dritte erfolgt nur in Absprache mit dem Kunden oder gemäß Weisung des Kunden/der vertraglichen Vereinbarung bzw. der gesetzlichen Notwendigkeit.

5) Eingabekontrolle

Es werden Systeme mit Protokollfunktionen für relevante Daten eingesetzt. Protokolle werden entsprechend Standards bzw. gesetzlicher Vorgaben aufbewahrt.

6) Auftragskontrolle

Es erfolgt ein Evaluierungsverfahren zur Prüfung, Bewertung und Auswahl potentieller Kunden.

Eine eindeutige Vertragsgestaltung mit Abgrenzung der Rechte und Pflichten der Parteien wird mit formalisierten Verträgen und Auftragsformularen sichergestellt.

7) Verfügbarkeitskontrolle

Eine regelmäßige Datensicherung wird durchgeführt.

Gesetzliche Vorgaben zum Brand- und Wasserschutz werden in allen Gebäuden eingehalten.

Das Rechenzentrum ist ISO27001 und nach weiteren TÜV Standards zertifiziert und entspricht hohen Anforderungen an Brand- und Wasserschutz. Das Rechenzentrum ist durch getrennte USV-Anlagen mit Batteriepufferung und Dieselgenaratoren gegen Stromausfälle gesichert. Die Hauseinführung ist redundant implementiert.

Maßnahmen zum Schutz von Systemen und Umgebungen gegen unberechtigte Zugriffe, Viren und Malware sind im Gesamtumfeld definiert und implementiert

8) Trennungskontrolle

Die Daten werden ausschließlich gemäß den im Leistungsvertrag skizzierten Anforderungen zweckgebunden verarbeitet.

9) Datenschutz-Managementsystem

Datenschutzrelevante Verantwortungsbereiche werden je nach Tätigkeitsbereich auf Mitarbeiter verteilt. Dabei wird die Eignung der Mitarbeiter für den jeweiligen Verantwortungsbereich stets sichergestellt. Ggf. notwendige Schulungen oder Fortbildungen erfolgen vor der Übertragung eines Verantwortungsbereichs an einen Mitarbeiter. Bei Austritt eines Mitarbeiters wird unverzüglich ein geeigneter Nachfolger benannt.

Genehmigte Subunternehmer Erläuterungen

Unternehmen	Sitz	Tätigkeit
BT (Germany) GmbH & Co. oHG	Deutschland	Netzbetreiber
NorthC Deutschland GmbH	Deutschland	Rechenzentrumsdienstleister
Hetzner Online GmbH	Deutschland	Rechenzentrumsdienstleister
ALLNET GmbH Computersysteme	Deutschland	Hardware Distributor
Sage GmbH	Deutschland	Buchhaltungsdienstleister
Scavix Software GmbH & Co. KG	Deutschland	Softwaredienstleister
sipgate GmbH	Deutschland	VoIP-Anbieter
Designmodo Inc.	Spanien	Betreiber der Status Seite
Jetbrains s.r.o.	Tschechien	Softwaredienstleister
OpenAI Ireland Limited	Irland	KI-Dienstleister
Amazon Web Services EMEA SARL	Luxemburg	Storagedienstleister
Microsoft Ireland Operations, Ltd.	Irland	Softwaredienstleister
In-Tuition Networks Limited*	England	E-Maildienst
NUMB3RS Berlin Steuerberatungsgesellschaft mbH	Deutschland	Steuerberater
Sinch AB	Schweden	Softwaredienstleister
Nexmo Inc.*	USA	Rufnummerzulieferer
Wunschgutschein GmbH	Deutschland	Gutscheinvergabe
Sendinblue GmbH	Deutschland	Softwaredienstleister

**Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses nach DSGVO Art. 45*