Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Verantwortlicher - nachfolgend Auftraggeber genannt:

Organisation
Straße
PLZ Ort
Land

Auftragsverarbeiter - nachfolgend Auftragnehmer genannt:

SerNet Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen
Deutschland

Präambel

(1) In Ergänzung zu dem zwischen den Parteien geschlossenen Vertrag konkretisieren die Vertragsparteien in der vorliegenden Vereinbarung die beiderseitigen datenschutzrechtlichen Rechte und Pflichten. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(2) Sofern in diesem Vertrag die Begriffe „Daten“ oder „Verarbeitung“ erwähnt sind, werden die Definitionen des Art. 4 I u II DSGVO zugrunde gelegt. Auch im Übrigen wird auf die Begriffsbestimmungen des Art. 4 DSGVO verwiesen.

1. Vertragsgegenstand

sind verinice.cloud als Software as a Service (SaaS) und damit verbundenes Hosting und Dienstleistungen. Dabei ist der Zugriff auf personenbezogene Daten generell nicht ausgeschlossen.

(2) Die Bestimmungen dieses Vertrages 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 bzw. durch den Auftraggeber oder für den Auftraggeber erhoben wurden.

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

2. Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf personenbezogenen Daten:

- Verarbeitungsverzeichnisse mit internen Zuständigkeiten und Dokumentation weiterer Datenprozesse und IT-Sicherheitsaspekte:

- Funktionsbezeichnung
- IT-Nutzungsdaten
- Kontaktdaten
- Name, Vorname
- Planungsdaten

- Bei Hosting:
  - Zeiterfassungsdaten
  - Bilder
  - Nutzungs- und Bestandsdaten, Logfiles (IP-Adresse, Name, Vorname, Adresse, Online-Kennung)

(2) Der Kreis der von der Datenverarbeitung Betroffenen sind:

- Alle Nutzerinnen und Nutzer der SaaS
  - Mitarbeiterinnen und Mitarbeiter des Auftraggebers
  - Kundinnen und Kunden des Auftraggebers und deren Mitarbeiterinnen und Mitarbeiter

3. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO zu [Einzelheiten in Anlage 1: TOM].

(3) Zur Wahrung der Vertraulichkeit gemäß Art. 28 III S. 2 lit. b), 29, 32 IV DSGVO stellt der Auftragnehmer sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter zur Wahrung des Datengeheimnisses verpflichtet und mit den jeweiligen besonderen Erfordernissen des Datenschutzes durch entsprechende Schulungen vertraut gemacht wurden. Sie dürfen die Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer stellt ferner sicher, dass Kenntnisse von Geschäftsgeheimnissen und technischen und organisatorischen Maßnahmen des Auftraggebers vertraulich behandelt werden. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

4. Melde- und Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 – 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten

bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die Umstände und Zwecke der Verarbeitung, sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen.
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich informieren über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(3) 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.

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

(5) Für Unterstützungsleistungen, die einen Mehraufwand beim Auftragnehmer verursachen oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

5. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit eine Prüfung/Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 III lit. c), 32 DSGVO insbesondere in Verbindung mit Art. 5 I u. II DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 I DSGVO zu berücksichtigen (Einzelheiten in Anlage 1: TOM).

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

(4) Dem Auftraggeber entstehen durch die Fortentwicklung des Datenschutzniveaus keine gesonderten Kosten. Hierfür ist der Auftragnehmer alleine verantwortlich.

6. 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 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 im Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(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) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

7. Kontrollrechte und -pflichten des Auftraggebers

(1) Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen die Daten des Auftraggebers verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen.

(2) Zur Durchführung der Kontrolle muss der Auftragnehmer nur eine solche Person zulassen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse des Auftragnehmers und Sicherheitsmaßnahmen, verpflichtet ist. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen. Eine die Kontrolle im Namen des Auftraggebers durchführende Person muss mindestens eine Woche vor Durchführung der Kontrolle ihre Legitimation durch den Auftraggeber schriftlich oder per Telefax nachweisen.

(3) Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von schwerwiegenden Vorkommnissen durchzuführen.

(4) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

(5) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- oder aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz)

8. Subunternehmer

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt, sofern ausgeschlossen werden kann, dass der eingesetzte Dienstleister die Möglichkeit des Zugriffs auf die personenbezogenen Daten erhält. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter

besonderer Berücksichtigung der Eignung der von dieser getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(3) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(4) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde

gelegt wird.

(5) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(6) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(7) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Art. 28 Abs. 1 Satz 2 eingesetzt werden sollen.

(8) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform).

(9) Zur Zeit der Vertragsunterzeichnung arbeitet die Auftragnehmerin mit folgenden Rechenzentren als Unterauftragnehmerinnen zum Hosten der SaaS:

- Hostserver GmbH, Biegenstr. 20, 35037 Marburg, Deutschland
- SysEleven GmbH, Boxhagener Straße 80, 10245 Berlin, Deutschland

9. 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, 32 u. 36 DSGVO.

(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.

10. Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich. Der Auftragnehmer verpflichtet sich den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten unter Vereinbarung einer angemessenen Gebühr zu unterstützen.

(2) Der Auftragnehmer haftet im Innenverhältnis im Rahmen der gesetzlichen Bestimmungen nach Art. 82 II DSGVO für Schäden, die infolge schuldhaften Verhaltens gegen die Datenschutzbestimmungen oder gegen diese Datenschutzvereinbarung entstehen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

11. Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO 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 der der Auftragnehmer den Verstoß abstellen kann.

12. Beendigung des Hauptvertrags, Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Ende des Hauptvertrages oder früher nach Aufforderung durch den Auftraggeber hat der Auftragnehmer sämtliche Datenbestände einschließlich etwaiger in seinen Besitz gelangter Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewah-

rungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) 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. 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. Die Parteien vereinbaren, die ungültige Bestimmung durch eine solche zu ersetzen, die wirtschaftlich der Zielsetzung der Parteien am nächsten kommt. Gleiches gilt für Regelungslücken.

(4) Diese Vereinbarung unterliegt deutschem Recht. Als Gerichtsstand ist der Sitz des Auftraggebers vereinbart.

Göttingen, Datum	Ort, Datum
Unterschrift Auftragnehmer	*Unterschrift Auftraggeber*
Name, Funktion Auftragnehmer	*Name, Funktion Auftraggeber*

Anlage 1

TOM - Technisch-Organisatorische Maßnahmen der SerNet

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Dies sind Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Schlüssel plus Codekarte, dokumentierte Schlüssel- und Codekartenvergabe, abgeschlossene Sicherheitszonen im eigenen RZ, zu diesen Sicherheitszonen (Rechenzentrum, technische Räume) hat nur ein eingeschränkter MA-Kreis Zutritt (ausschließlich Festanstellungen), Dritte dürfen sich nur in Begleitung eines Mitarbeiters in Räumlichkeiten aufhalten, Einbruchmeldeanlage 24/7 bei Sicherheitsdienstleister aufgeschaltet, Brandmeldeanlage direkt zur Feuerwehr geschaltet, Monitoring aller Rechner-Systeme 24/7 mit abgestufter, redundanter Alarmierung (Rufbereitschaft) sowohl für Kunden als auch für eigene Belange.

1.2 Zugangskontrolle

Dies sind Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und Datenverarbeitungsverfahren benutzen können (z. B. Firewall / Verschlüsselungsverfahren entsprechend dem Stand der Technik).

Intern beim AN: Zertifikatsbasierte Zugriffskontrolle, SUDO-basierter Zugriff auf Admin-Schnittstellen inkl. Logging der Zugriffe. Einsatz von Anti-Viren-Software, Firewalls, VPN mit 2FA. Passwortregeln, Festlegung und Verwaltung von Benutzerberechtigungen, Identifikation und Authentifizierung von Benutzern.

Bei Hauptauftrag: Support wird mit den zwischen Auftragnehmer und Auftraggeber vereinbarten VPN-Techniken umgesetzt.

1.3 Zugriffskontrolle

Dies sind Maßnahmen, die gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungsverfahren Befugten auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

Intern beim AN: Rollenbasiertes Berechtigungssystem, Protokollierung der Systemnutzung, Umsetzung des Need-to-know Prinzips.

Bei Hauptauftrag: Dem Auftragsumfang entsprechend werden die Zugriffsrechte des Wartungspersonals vergeben.

1.4 Trennungskontrolle

Dies sind Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Intern bei AN: Trennung von technischen Daten, Vertragsdaten und kaufmännischen Daten mit definierter Rechtestruktur.

Bei Hauptauftrag: Die Speicherung der Daten erfolgt pro Kunde/Mandant in jeweils eigenen „Tenants“. Diese Tenants sind streng voneinander getrennt und ein Übergreifen von Zugriffen zwischen verschiedenen Tenants wird technisch unterbunden.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Dies sind Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Intern beim AN: Schriftliche Regelung zum Verbot der Weitergabe personenbezogener oder unternehmensbezogener Daten, E-Mail Verschlüsselung (GPG, S/MIME), getrennte Wege zur Kennwortübermittlung, Datentransfer über gesicherte Webverbindung (SSL/SFTP), Festplattenverschlüsselung, Verschlüsselung von Datenträgern, VPN-Einsatz mit 2FA, automatische Eskalation bei Sicherheitsmeldungen, gesicherter Medientransport, Regelungen zur sicheren Aufbewahrung und Vernichtung, z.B. Einsatz von Aktenvernichtungsgeräten etc.

Bei Hauptauftrag: Grundsätzlich verbleiben die Daten vollständig beim Auftraggeber, sofern sie nicht auf den Systemen des Auftragnehmers und dessen Unterauftragnehmer verarbeitet werden. Der Datentransfer erfolgt immer über gesicherte Verbindungen (SSL). Die Daten der Kunden liegen unverschlüsselt in den Datenbanken der Unterauftragnehmer (Rechenzentren).

2.2 Eingabekontrolle

Dies sind Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingesehen, eingegeben, verändert oder entfernt worden sind.

Intern beim AN: Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind – soweit technisch möglich.

Bei Hauptauftrag: Die zu verarbeitenden Daten werden durch den Auftraggeber selbst erfasst und auf eigenen Systemen oder Systemen der Auftragnehmer und Unterauftragnehmer verarbeitet und gespeichert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Dies sind Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, z.B. Maßnahmen zur Datensicherung (physikalisch / logisch).

Intern bei AN: Backups, USV, Notfallplan, Virenschutz, Firewall, Aufbewahrung physischer Dokumente in abgeschlossenen Schränken, abgesetzter Speicherort aller Daten in mehreren Kilometern Entfernung zum Firmensitz im geschützten RZ per Glasfaser. Redundante Hochverfügbarkeit (z.B. DNS) zusätzlich an verteilten Standorten in Deutschland und im Ausland.

Bei Hauptauftrag: Der Kunde ist für die Sicherung der von ihm eingegebenen Daten selbst zuständig. Dafür bietet die Anwendung einfache Exportmöglichkeiten für die Datenbanken des Kunden an. Über ein Revisionsprotokoll sind Änderungen an Daten auch über die Anwendung auf Feldebene nachvollziehbar und können über die Anwendung zurück gesetzt werden .

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Intern beim AN: Datenschutzrelevante Prozesse im Unternehmen werden definiert und regelmäßig überprüft, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Verantwortlichkeiten und Zuständigkeiten im Bereich Datenschutz und Informationssicherheit sind festgelegt und wurden den Mitarbeitern zur Kenntnis gebracht. Die erforderliche berufliche Qualifikation und Fachkunde der Datenschutzbeauftragten wird durch regelmässige Fortbildungsmöglichkeiten gewährleistet.

Die Steuerung des Datenschutzmanagements erfolgt durch regelmäßigen Jour-Fixes mit den Beauftragten für Datenschutz, Informationssicherheit und der Geschäftsleitung, um einen kontinuierlichen Verbesserungsprozess sicherzustellen. Durch regelmäßig angesetzte interne Audits erfolgt eine Überprüfung der technisch organisatorischen Maßnahmen sowie der unternehmensspezifischen Anforderungen und Regelungen.

Abweichungen werden mit dem Ziel analysiert, das Datenschutz-Niveau anzugleichen bzw. kontinuierlich zu verbessern.

4.2 Incident-Response-Management

Intern beim AN: Incident-Response-Management eingerichtet, festgelegte Vorgehensweise zum Umgang mit Sicherheitsvorfällen, Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen, festgelegte Prüfroutine, Implementierung von Verbesserungsvorschlägen. Betrieb eines Ticket-Systems zur Verwaltung, Bearbeitung, Wiedervorlage und Dokumentation der Vorgänge. Betrieb eines Monitoring-Systems zur automatischen Störungs-Aufnahme und Verarbeitung, Kopplung von Ticket-System und Monitoring. Ausführliche Dokumentation aller technischen Systeme.

4.3 Auftragskontrolle

Intern beim AN: Bei der Betreuung eigener IT-Systeme des Auftragnehmers werden Dienstleister beauftragt, die zwar keinen Zugriff auf personenbezogene Daten des Auftraggebers bekommen, jedoch folgender Sorgfalt bei der Auswahl unterliegen: Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit), vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen, schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag), Verpflichtung des Dienstleisters auf Vertraulichkeit, wirksame Kontrollrechte gegenüber dem Dienstleister, regelmäßige Überprüfung des Dienstleisters und seiner Tätigkeiten.

Bei Hauptauftrag: Grundsätzlich verarbeitet die SerNet die ihr überlassenen Daten nur aufgrund und anhand der vertraglich vereinbarten Weisungen ihrer Auftraggeber. Kompeten-

zen und Kontrollmaßnahmen werden in Abstimmung mit den Auftraggebern definiert und technisch oder organisatorisch in die Betriebsabläufe eingebunden.

5. Die innerbetriebliche Organisation

Die innerbetriebliche Organisation ist durch geeignete Maßnahmen so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Maßnahmen zur Organisationskontrolle: Regelmäßige Schulungsmaßnahmen der Mitarbeiter zu Datenschutz und Datensicherheit, alle Mitarbeiter sind auf Vertraulichkeit, das Datengeheimnis und auf das Fernmeldegeheimnis verpflichtet. Es erfolgen regelmäßige Hinweise und Schulungen, um das Problembewusstsein zu fördern, sowie gelegentliche nicht angekündigte Kontrollen der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen.

Externe Datenschutzbeauftragte beim Auftragnehmer:

RAin Johanna Feuerhake
Obere-Masch-Straße 22, 37073 Göttingen
Tel.: +49-551-5311924
E-Mail: datenschutz@sernet.de