Zusatzbedingungen Datenschutz - Auftragsverarbeitung

Zusatzbedingungen Datenschutz zur Auftragsverarbeitung im Rahmen des Produkts enGiga Secure bzw. enManaged Firewall zwischen dem Kunden (Auftraggeber) und envia TEL GmbH (Auftragnehmer).
Die Verarbeitung personenbezogener Daten erfolgt im Rahmen einer Auftragsverarbeitung (AV) im Sinne des Art. 4 Nr. 8 i. V. m. Art. 28 EU DSGVO.

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem zugehörigen Vertrag zu enGiga Secure bzw. enManaged Firewall (im Folgenden Produkt) bezüglich folgender beauftragter Leistung: IT-Sicherheitsdienstleistungen.

1.2 Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Kundenvertrags.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ist die Bereitstellung von IT-Sicherheitsdienstleistungen. Dies umfasst Tätigkeiten, die in der Leistungsvereinbarung und den dazugehörigen Anlagen konkret beschrieben sind.
Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

2.2 Ort der Leistungserbringung

Die Erbringung der vertraglich vereinbarten Leistung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.3 Art der Daten

Gegenstand der, Verarbeitung personenbezogener Daten sind sämtliche Datenarten/-kategorien aus dem elektronischen Datenverkehr der betreuten/bereitgestellten Dienste/Systeme gem. Kundenvertrag sowie organisatorisch erforderliche Daten zur Vertragserfüllung. Dies umfasst unter anderem:

- Vertragsstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- TK-Daten (Verkehrs-, Standort,- und Bestandsdaten, Einzelverbindungsdaten)
- Telemediendaten (Nutzungs- und Bestandsdaten) oder elektronische Kommunikationsdaten (elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten)
- Besondere Arten personenbezogener Daten (z.B. über Nutzungsinhalte)

2.4 Kategorien betroffener Personen

Die durch die Verarbeitung der Daten betroffenen Personen umfasst sämtliche Personen, die den elektronischen Datenverkehr der betreuten/bereitgestellten Dienste/Systeme gem. Kundenvertrag in Anspruch nehmen. Dies umfasst unter anderem:

- Mitarbeiter
- Kunden

3 Technische- und organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i. V. m. RiLi 2009/136/EG vor der Auftragserteilung und 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 die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, Art. 32 DSGVO insbesondere in Verbindung mit Art. 5
Abs. 1, Abs. 2 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 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anlage „Technisch-Organisatorische Maßnahmen enGiga Secure“).
Er verpflichtet sich zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i. V. m. RiLi 2009/136/EG: Die als Anlage beigefügten „Technisch-Organistorische Maßnahmen enGiga Secure“ werden für den Auftragnehmer als verbindlich festgelegt.
Anstelle der als Anlage beigefügten „Technisch-Organisatorische Maßnahmen enGiga Secure“ kann der Auftragnehmer in Ausnahmefällen nach Abstimmung mit dem Auftraggeber eine auftragsbezogene Dokumentation der technischen und organisatorischen Maßnahmen vornehmen.
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 Sicherheits-

envia TEL GmbH
Geschäftsanschrift Friedrich-Ebert-Straße 26 · 04416 Markkleeberg · T 0800 0101600 · F 0800 3684283
www.enviaTEL.de · info@enviaTEL.de · **Geschäftsführung** Stephan Drescher · **Sitz der Gesellschaft** Markkleeberg
Registergericht Amtsgericht Leipzig · HRB 24812 · **USt-ID-Nr.** DE183563546

Ein Unternehmen der enviaM-Gruppe

niveau der festgelegten Maßnahmen nicht unterschritten werden.

4 Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken, mit Ausnahme der Regelungen unter Punkt 11 dieser Zusatzbedingungen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
a) Der Auftragnehmer hat einen Datenschutzbeauftragten benannt. Die Kontaktdaten sind unter www.enviatel.de jederzeit abrufbar.
b) Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO und/oder des etwaig gesetzlich bestehenden Fernmeldegeheimnisses sowie Wahrung der Vertraulichkeit elektronischer Kommunikationsdaten. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese 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. Die sich daraus ergebende Geheimhaltungspflicht gilt über das Vertragsende auf unbefristete Zeit hinaus, unabhängig von der Regelung über sonstige Geheimhaltungspflichten. Gleiches gilt für Daten, die dem Fernmeldegeheimnis unterliegen.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO sowie, wenn zutreffend, der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i. V. m. RiLi 2009/136/EG.
d) Auf Verlangen der Aufsichtsbehörde arbeiten der Auftraggeber und der Auftragnehmer bei der Erfüllung von deren Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Auftragsverarbeitungs-Vertrages.
j) Der Auftragnehmer setzt bei Notwendigkeit mobilen Arbeitens nur Mitarbeiter und Erfüllungsgehilfen ein, die zum Arbeiten außerhalb von Betriebsstätten des Auftragnehmers gesondert belehrt und verpflichtet werden.

6 Unterauftragsverhältnisse

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 als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen. Folgende Unterauftragnehmer hat der Auftragnehmer nach Maßgabe des Art. 28 Abs. 2-4 DSGVO verpflichtet:

Firma-Unterauftragnehmer	Drittlandübermittlung	Leistung
CCL Call- und Servicecenter Lausitz GmbH	nein	Callcenter
magellan netzwerke GmbH	nein	Auftragsbearbeitung, Betriebsunterstützung

Zusatzbedingungen Datenschutz - Auftragsverarbeitung

Der Wechsel des bestehenden Unterauftragnehmers ist 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 DSGVO zugrunde gelegt wird.

7 Weisungsberechtigte Person auf Seiten des Auftraggebers

Der Auftraggeber benennt dem Auftragnehmer mit der Bestellung des Produkts mindestens eine weisungsberechtigte Person, die auch als Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen fungiert und bei Bedarf einen Kontakt zum Datenschutzbeauftragten des Auftraggebers herstellt. Einen Wechsel einer/der weisungsberechtigten Person(en) wird der Auftraggeber dem Auftragnehmer unverzüglich schriftlich mitteilen.

8 Kontrollrechte des Auftraggebers

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.
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.
Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann vorrangig erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutz beauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach einem ISO 27001).

9 Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der 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 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 (einschließlich Fälle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung) personenbezogener Daten des Auftraggebers ohne Ansehen der Verursachung unverzüglich an den Auftraggeber zu melden.
c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber der betroffenen Person zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante 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.

10 Weisungsbefugnis des Auftraggebers

Der Auftraggeber erteilt Weisungen grundsätzlich schriftlich, mindestens in Textform. Sofern eine Weisung des Auftraggebers nur mündlich erteilt wird, wird der Auftragnehmer die Bestätigung mindestens in Textform beim Auftraggeber anfordern. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.
Ziffer 5 lit. c) Satz 3 dieser Auftragsverarbeitungs-Vereinbarung bleibt unberührt.
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.

11 Löschung von Daten und Rückgabe von Datenträgern

Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und 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.
Nach Abschluss der vertraglichen Arbeiten oder nach Aufforderung durch den Auftraggeber – spätestens jedoch mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung/Ver-

nichtung ist dem Auftraggeber auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.