# VEREINBARUNG ZUR VERARBEITUNG PERSONENBEZOGENER DATEN IM AUFTRAG (Auftragsverarbeitung gem. Artikel 28 DS-GVO)

zwischen

**Partner**

Adresse

im Folgenden **Auftraggeber**

und

reev GmbH

Sandstr. 3

80335 München

im Folgenden **Auftragnehmer**

## 1 Gegenstand und Dauer des Auftrags

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

1.2 Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung über die Erbringung von Dienstleistungen, beginnend mit Unterzeichnung dieser, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung). Der Auftrag kann im Bedarfsfall durch Einzelaufträge erweitert werden.

1.3 Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung. Diese Vereinbarung zur Auftragsverarbeitung wird automatisch Bestandteil sämtlicher in Ziffer 1 Absatz 2 bezeichneten Einzelaufträge und ergänzt diese. Diese Vereinbarung geht den datenschutzrechtlichen Regelungen der Einzelaufträge vor.

## 2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in der Leistungsvereinbarung vom Dienstleistungsvertrag sowie in den darauf aufsetzenden jeweiligen Angeboten/Verträgen beschrieben.

2.2 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Mitgliedsstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Das angemessene Schutzniveau kann wie folgt hergestellt werden:

- durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);
- durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);
- durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. C und d DSGVO);
- durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);
- durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).
- durch sonstige Maßnahmen:

  Der Auftragnehmer arbeitet ausschließlich auf den vom Auftraggeber zur Verfügung gestellten Systemen und speichert keine Daten ab. (Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DSGVO).

2.3 Bei Bedarf werden Datentransfer-Folgenabschätzung im Rahmen der Verarbeitung personenbezogener Daten in unsicheren Drittländern durchgeführt.

# 3 Art der Daten und betroffene Personengruppen

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

| **Art der Daten** | **Zweck der Datenerhebung, -verarbeitung oder -nutzung** | **Kreis der Betroffenen** |
|---|---|---|
| Name (Vorname, Nachname)<br>Email-Adresse<br>Telefonnummer (geschäftlich) – optional<br>Name des Unternehmens des Partners<br>Standort des Unternehmens des Partners | Zur Vertragserfüllung: Anlage Benutzerkonto und Identifikation bei Passwortübermittlung | • Mitarbeiter mit Zugriff auf Verwaltungsoberfläche |
| Name (Vorname, Nachname)<br>Email-Adresse<br>Telefonnummer (geschäftlich)<br>Name des Unternehmens des Partners<br>Standort des Unternehmens des Partners | Zur Vertragserfüllung: Erstellung der eindeutigen Kennung des Partners | • Mitarbeiter mit Zugriff auf Verwaltungsoberfläche |
| Name (Vorname, Nachname)<br>Email-Adresse<br>Telefonnummer (geschäftlich)<br>Name des Unternehmens des Partners<br>Standort des Unternehmens des Partners | Zur Vertragserfüllung: Übermittlung von Kontaktdaten des Partners an den Kunden | • Mitarbeiter mit Zugriff auf Verwaltungsoberfläche |

# 4 Pflichten des Auftragnehmers

## 4.1 Technisch-organisatorische Maßnahmen

4.1.1 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 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.

4.1.2 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.

4.1.3 Die Zusammenfassung der aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers ist dieser Vereinbarung als **Anlage** beigefügt, mit denen sich der Auftraggeber einverstanden erklärt.

## 4.2 Unterstützungspflicht

4.2.1 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers sowie 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 hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen. Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten. Hierzu gehören u.a.

4.2.1.1 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

4.2.1.2 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

4.2.1.3 die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

4.2.1.4 die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

4.2.1.5 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

4.2.1.6 Informationen unverzüglich zur Verfügung zu stellen

4.2.1.7 die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

4.2.1.8 die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

4.2.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind und über die gesetzlichen Pflichten des Auftragnehmers hinausgehen, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Hinsichtlich der Vergütungshöhe wird auf die entsprechende Vergütungsklausel verwiesen.

### 4.3 Verarbeitung personenbezogener Daten im Home- bzw. Mobile-Office

4.3.1 Der Auftraggeber stimmt der Verarbeitung von Daten außerhalb der Betriebsräume (z.B. Telearbeit, Heimarbeit, Home-Office, mobiles Arbeiten) zu. Der Auftragnehmer verpflichtet sich:

4.3.2 zur Unterstützung seiner Beschäftigten bei der Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen in ihren privaten Räumlichkeiten, um die Sicherheit der Daten zu garantieren.

4.3.3 zur angemessenen Unterrichtung seiner Beschäftigten bezüglich der Einhaltung der technischen und organisatorischen Maßnahmen und sonstigen Sorgfaltspflichten, die es bei der Verarbeitung der Daten in privaten Räumlichkeiten einzuhalten gilt.

## 5 Sonstige Pflichten des Auftragnehmers

5.1 Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

5.2 Der Auftragnehmer gewährleistet die Bereitstellung eines Datenschutzbeauftragten:

Als Datenschutzbeauftragte ist beim Auftragnehmer SiDIT GmbH, info@sidit.de, Tel: +49 931 78 08 77 - 0 bestellt. Ein Wechsel des Datenschutzbeauftragten wird in der Datenschutzerklärung kenntlich gemacht.

5.3 Der Auftragnehmer gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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. Diese Vertraulichkeitsverpflichtung der Mitarbeiter gilt auch nach Beendigung ihres jeweiligen Arbeitsvertrages fort.

5.4 Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5 Der Auftragnehmer gewährleistet 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.

5.6 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. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind und über die gesetzlichen Pflichten des Auftragnehmers hinausgehen, kann der Auftragnehmer eine angemessene Vergütung beanspruchen.

5.7 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.

# 6 Pflichten und Rechte des Auftraggebers

## 6.1 Verantwortlichkeit

6.1.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

6.1.2 Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

## 6.2 Weisungsbefugnis

6.2.1 Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

6.2.2 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. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den

Auftraggeber weiterleiten. Sofern technisch und nach dem Zweck der Leistungsvereinbarung erforderlich, darf der Auftragnehmer Daten von Geräten auch ohne diesbezügliche Weisung löschen (z.B. bei einem schnell erforderlichen, technisch notwendigen Austausch eines Gerätes). Entstehen dem Auftragnehmer Kosten bei Löschung der Daten, so trägt diese der Auftraggeber.

6.2.3 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

6.2.4 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.

## 6.3 Kontrollrechte

6.3.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen zur Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Dem Auftragnehmer steht es frei, zur Erfüllung dieses Überprüfungsrechts dem Auftraggeber entsprechende Kontrollberichte oder ähnliche Dokumentationen, die eine datenschutzkonforme Datenverarbeitung belegen, vorzulegen. Soweit dem Auftraggeber Zweifel an der Datenschutzkonformität der Datenverarbeitungen verbleiben, hat er 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.

6.3.2 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.

6.3.3 Der Auftragnehmer ist berechtigt, den Nachweis solcher Maßnahmen zu erbringen, die nicht nur den konkreten Auftrag betreffen, durch

6.3.3.1 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

6.3.3.2 die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

6.3.3.3 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

6.3.3.4 eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

6.3.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Als angemessen gilt die Abrechnung des entstandenen Aufwands nach den vom Auftragnehmer üblicherweise verlangten Stundensätzen.

## 7 Unterauftragsverhältnisse

7.1 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 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.

7.2 Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mindestens vier Wochen vor dem geplanten Wechsel schriftlich oder in Textform anzeigt und der Auftraggeber nicht innerhalb von 2 Wochen ab Zugang der Mitteilung gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt. Der Auftragnehmer wird mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO schließen. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

7.3 Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

| Name und Anschrift des Subunternehmers | Beschreibung der Teilleistungen |
|---|---|
| AWS - Amazon Web Services, Inc.<br>410 Terry Avenue North<br>Seattle WA 98109<br>United States | Server Hosting (Europa) |

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

7.5 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 Abs. 1 Satz 2 eingesetzt werden sollen.

## 8 Löschung und Rückgabe von personenbezogenen Daten

8.1 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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 ist auf Anforderung vorzulegen. Entstehen dem Auftragnehmer Kosten bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

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

## 9 Haftung und Schadensersatz

9.1 Der Auftraggeber gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen bei der Verarbeitung personenbezogener Daten.

9.2 Es gelten grundsätzlich die Haftungsbeschränkungen aus dem Hauptvertrag. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer auf Grund der vom Auftraggeber beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten

auf einer rechtswidrigen Verarbeitung der personenbezogenen Daten durch den Auftragnehmer beruht. Art. 82 DSGVO bleibt unberührt.

## 10 Sonstiges, Allgemeines

10.1 Sollten die personenbezogenen 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

10.2 Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des primären Leistungsverhältnisses bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

10.3 Sollten einzelne Teile der hier vorliegenden Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit dieser Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt.

_____ _____

Ort, Datum Unterschrift Auftraggeber

_____ _____

Ort, Datum Unterschrift Auftragnehmer

(Reviewed in January 2025)

# Anlage 1 zur AV-Vereinbarung:

# Allgemeine technische und organisatorische Maßnahmen

gemäß Art. 32 Abs. 1 DSGVO

# 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

## 1.1. Zutrittskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern:

- Klingelanlage mit Kamera
- Chipkarten / Transpondersysteme
- Türen mit Knauf an der Außenseite
- Schlüsselregelung / Schlüsselbuch
- Ausweis-Vergaberegelung
- Token-Vergaberegelung
- Besucher / Externe in Begleitung durch Mitarbeiter
- Externer Reinigungsdienst
- Externer Wartungsdienst
- Maßnahmen bei Verlust von Schlüssel / Ausweis / Dongle / Token/ Chipkarte

## 1.2. Zugangskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zugang zu den Datenverarbeitungssystemen zu verhindern:

- Login mit Benutzername + Passwort
- Login mit biometrischen Daten
- Anti-Virus-Software Clients
- Firewall - Server
- Externer Zugang durch Mobile- / Homeoffice (bspw. PC / Laptop)
- Externer Zugang von externen Dienstleistern
- Externer Zugang durch Smartphones /Tablets
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablet
- Verschlüsselung bei WLAN-Benutzung (WPA2)
- Erstellen und Verwalten von Benutzerprofilen und -berechtigungen
- Anleitung „Manuelle Desktopsperre“
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen / Vernichten“
- Richtlinie „Clean desk“
- Richtlinie "Home-/Mobile-Office"
- Mobile Device Policy

## 1.3. Zugriffskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten das Lesen, Kopieren, Verändern oder Löschen innerhalb der Datenverarbeitungssysteme zu verhindern:

- Aktenschredder
- Externer Aktenvernichter
- Physische Löschung von Datenträgern
- Berechtigungskonzept(e)
- Minimale Anzahl an Administratoren
- Datenschutztresor
- Verwaltung Benutzerrechte durch Administratoren

### 1.4. Trennungskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten zu trennen:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Bedarfsgerechte Zugriffsberechtigungen der Mitarbeiter
- Festlegung von Datenbankrechten

### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) & Art. 25 Abs. 1 DSGVO)

Die Pseudonymisierung von Datensätzen wird durch folgende Maßnahmen umgesetzt:

Es findet keine Pseudonymisierung der Datensätze statt.

## 2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

### 2.1. Weitergabekontrolle

Personenbezogene Daten müssen bei der elektronischen Übermittlung ausreichend geschützt werden, um nicht unbefugt gelesen, kopiert, verändert oder entfernt zu werden. Folgende technische und organisatorische Maßnahmen haben wir hierfür ergriffen:

- Email-Verschlüsselung
- Bereitstellung von Tunnelverbindungen (VPN)
- Bereitstellung verschlüsselter Verbindungen
- Elektronische Signaturverfahren
- Protokollierung der Zugriffe und Abrufe in Log-Dateien
- Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen

### 2.2. Eingabekontrolle

Zur Kontrolle, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, geändert, gesperrt oder gelöscht werden, setzen wir folgende Maßnahmen ein:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten

- Manuelle oder automatisierte Kontrolle der Protokolle
- Softwareliste mit Datenverarbeitungsprogrammen
- Vergabe individueller Benutzernamen
- Berechtigungskonzept mit Vergabe von bedarfsgerechten Benutzerrechten
- Sichere Aufbewahrung von Dokumenten in Papierform

# 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

## 3.1. Verfügbarkeitskontrolle

Zur Gewährleistung der Verfügbarkeit personenbezogener Daten gegen zufällige oder mutwillige Zerstörung oder Verlust, setzen wir folgende Maßnahmen ein:

- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

Die rasche Wiederherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. c) DSGVO) gewährleisten wir durch folgende Maßnahmen:

# 4. Verfahren zur regelmäßigen Überwachung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d) DSGVO & Art. 25 Abs. 1 DSGVO)

Datum der Evaluierung der technischen und organisatorischen Maßnahmen:

- 17.11.2022

## 4.1. Datenschutz-Management

Zur Gewährleistung des Datenschutzes in unserem Unternehmen setzen wir folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung ein:

- Softwarelösungen für Datenschutz-Management im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind.  jährlich durchgeführt
- Externer Datenschutzbeauftragter: Iris Duch, SiDIT GmbH, info@sidit.de
- Interner Informationssicherheitsbeauftragter: José Carvalho, reev GmbH, josé.carvalho@reev.com
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich

- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunfts-, Löschungs- und Datenübertragungsanfragen seitens Betroffener

## 4.2. Incident-Response-Management (gemäß Art. 33 DSGVO)

Im Falle des Erkennens und der Meldung von Datenschutzverletzungen setzen wir folgende Maßnahmen ein:

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB in Sicherheitsvorfällen und Datenpannen
- Einbindung von ISB in Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

## 4.3. Datenschutzfreundliche Voreinstellungen

Im Rahmen datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO) setzen wir folgende Maßnahmen ein:

- Datenminimierung und Zweckbindung
- Einfache (technische) Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

## 4.4. Auftragskontrolle (Outsourcing)

Im Rahmen des Outsourcings der Verarbeitung personenbezogener Daten durch Auftragsverarbeiter setzen wir für die Gewährleistung eines angemessenen Schutzniveaus folgende Maßnahmen ein:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfalts-Gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer

- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

(Reviewed in December 2024)