Vereinbarung zur Auftragsverarbeitung

Nach Art. 28 Abs. 3 DSGVO | Version 1.1 · 02.11.2026 | Kundenformular für Softwareentwicklung, WordPress, Remote-Support und VM-Mitnutzung

Verantwortlicher (Auftraggeber / Kunde)

Firma/Name: _____

Anschrift: _____

Kontakt / E-Mail: _____

Auftragsverarbeiter (genau einen Vertragspartner auswählen):

■ Itlerhilfe OÜ, Lootsa tn 2a, 11415 Tallinn, Estland; Registrierungsnummer 16614738; vertreten durch Geschäftsführer Ing. Klaus Schlender.

■ Quantum Solution – Klaus Schlender, freiberuflicher Informatiker; Geschäftsanschrift: _____ (vor Unterzeichnung bestätigen).

Die Anbieter sind rechtlich eigenständig. Nur der ausgewählte Anbieter wird Vertragspartner. Wird der andere Anbieter für die Verarbeitung von Kundendaten hinzugezogen, gelten § 7 und Anlage 3.

Hauptvertrag / Projekt / Website: _____ Datum: _____

§ 1 Gegenstand, Art und Dauer

1. Gegenstand sind die im Hauptvertrag vereinbarten Arbeiten, insbesondere Entwicklung und Anpassung von Software, Prototypen und Frameworks, WordPress-Einrichtung, Migration, Fehleranalyse, Wartung, Remote-Support sowie gegebenenfalls die Mitnutzung vorhandener Serverkapazitäten. Umfang und Betriebsart ergeben sich aus Anlage 1.

2. Die Servermitnutzung erfolgt regelmäßig über eine einem Kunden zugeordnete virtuelle Maschine (VM), auf der Website, Anwendung oder Framework betrieben werden und auf die eine Domain zeigt. Eine VM-Mitnutzung beinhaltet ohne gesonderte Vereinbarung weder einen vollumfänglichen Managed-Hosting-Dienst noch garantierte Anwendungsbetreuung, Datensicherung, Wiederherstellung oder Verfügbarkeit.

3. Die Verarbeitung umfasst je nach Auftrag Speichern, Bereitstellen, Testen, Ändern, Auslesen, Übermitteln, Sichern und Löschen. Der Kunde legt Zwecke und wesentliche Mittel fest. Die AVV gilt für die Dauer der beauftragten Verarbeitung bis zur Rückgabe/Löschung nach § 11.

§ 2 Verantwortung und Weisungen

1. Der Kunde ist verantwortlich für Rechtsgrundlagen, Datenschutzhinweise, erlaubte Inhalte, Rechte Betroffener und die Bewertung des Sicherheitsbedarfs seines Systems. Für kundenseitig administrierte Software und Plugins sorgt er grundsätzlich selbst für die notwendigen Konfigurationen und Maßnahmen, sofern dies nicht ausdrücklich beauftragt ist.

2. Verarbeitung erfolgt nur auf dokumentierte Weisung (Hauptvertrag, E-Mail, Ticket, freigegebene Anforderung), sofern keine zwingende gesetzliche Pflicht besteht. Bei einer solchen Pflicht informiert der Auftragsverarbeiter vorab, soweit rechtlich zulässig.

3. Der Auftragsverarbeiter weist unverzüglich auf nach seiner Auffassung rechtswidrige Weisungen hin und kann deren Ausführung bis zur Klärung aussetzen. Weisungsberechtigte Person des Kunden: _____.

§ 3 Vertraulichkeit und Personal

Zugriff erhalten nur berechtigte Personen, die zur Vertraulichkeit verpflichtet oder gesetzlich entsprechend gebunden sind. Für Homeoffice, Fernwartung und mobiles Arbeiten gelten dokumentierte Anforderungen an Geräteschutz, Zugriffsbeschränkung, sichere Übertragung und Vorfallmeldung. Eine interne Homeoffice-Verpflichtung ergänzt, ersetzt aber nicht diese AVV.

§ 4 Technische und organisatorische Maßnahmen (TOM)

1. Der Auftragsverarbeiter setzt angemessene Maßnahmen nach Art. 32 DSGVO für die von ihm kontrollierte Infrastruktur und Verarbeitung um. Anlage 2 ist vor Unterzeichnung auf den tatsächlich implementierten Stand anzupassen. Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellbarkeit sind risikobasiert zu bestimmen.

2. Die Parteien unterscheiden die Sicherheit der zugrunde liegenden Server-/VM-Infrastruktur von Sicherungs- und Betriebsmaßnahmen innerhalb der Kundenanwendung. Der Kunde bleibt für ihm zugewiesene Backup- und Betriebsaufgaben verantwortlich; dies entbindet den Auftragsverarbeiter nicht von seinen eigenen zwingenden Datenschutz- und Sicherheitsverpflichtungen.

3. Änderungen der Maßnahmen sind zulässig, sofern das vereinbarte Schutzniveau nicht wesentlich unterschritten wird. Zusätzliche Schutzmaßnahmen für sensible Daten oder produktive Systeme sind vor der Nutzung schriftlich festzulegen.

§ 5 Mitwirkung und Betroffenenrechte

Der Auftragsverarbeiter unterstützt den Kunden im Rahmen des Möglichen und unter Berücksichtigung der Art der Verarbeitung bei Anfragen betroffener Personen sowie bei Anforderungen nach Art. 32 bis 36 DSGVO. Unmittelbar eingehende Anfragen werden ohne eigenständige Entscheidung weitergeleitet, soweit rechtlich zulässig.

§ 6 Sicherheitsvorfälle

Bekannt gewordene Verletzungen des Schutzes personenbezogener Daten werden dem Kunden unverzüglich mitgeteilt; angestrebt wird eine Erstinformation innerhalb von 24 Stunden. Verfügbare Angaben zu Ereignis, betroffenen Daten, möglichen Folgen und Gegenmaßnahmen werden bereitgestellt und nachgereicht. Meldepflichten des Verantwortlichen bleiben bestehen.

§ 7 Unterauftragsverarbeiter

1. Externe Auftragsverarbeiter dürfen nur mit vorheriger besonderer oder allgemeiner schriftlicher Genehmigung nach Anlage 3 eingesetzt werden. Bei allgemeiner Genehmigung werden Änderungen grundsätzlich 14 Kalendertage vorher mitgeteilt; der Kunde kann aus Datenschutzgründen widersprechen.

2. Unterauftragsverarbeiter werden vertraglich auf angemessene Pflichten verpflichtet. Der beauftragte Hauptanbieter bleibt für deren Pflichterfüllung nach Art. 28 DSGVO verantwortlich.

3. Soweit Quantum Solution eigenständig für die Itlerhilfe OÜ Entwicklung, Administration oder Betreuung mit Zugriff auf Kundendaten ausführt, ist dies in Anlage 3 zu genehmigen; umgekehrt gilt dasselbe. Das persönliche Eigentum von Klaus Schlender an den Räumen allein begründet keine Unterauftragsverarbeitung.

§ 8 Serverstandort, Drittlandzugriffe

1. Die selbst betriebene Serverhardware befindet sich, soweit projektbezogen genutzt, in Graudenzer Weg 10, 32339 Espelkamp, Deutschland. Die Räumlichkeiten stehen im Eigentum von Klaus Schlender, der dort auch als freiberuflicher Informatiker tätig ist.

2. Der lokale Standort bedeutet nicht, dass externe Dienste, Domain/DNS, E-Mail, Supporttools oder vom Kunden ausgewählte Backup-Ziele dort liegen. Remote-Arbeit innerhalb der EU/des EWR ist bei angemessener Absicherung zulässig. Drittlandübermittlungen bedürfen der dokumentierten Weisung, geeigneter Garantien nach Kapitel V

DSGVO und einer entsprechenden Dokumentation.

§ 9 Nachweise und Prüfungen

Der Auftragsverarbeiter stellt erforderliche Nachweise zur Verfügung und ermöglicht angemessene Kontrollen nach Art. 28 Abs. 3 lit. h DSGVO. Vor-Ort-Prüfungen werden unter Wahrung von Schutzrechten anderer Kunden und Betriebsgeheimnissen koordiniert; gesetzlich erforderliche Kontrollrechte bleiben unangetastet.

§ 10 Prototypen, VM-Nutzung, WordPress und Backups

1. **Entwicklungsschwerpunkt:** Im Regelfall werden zunächst Prototypen, Test- oder Staging-Systeme erstellt. Es sollen soweit möglich Testdaten oder anonymisierte Daten verwendet werden. Prototypen sind ohne ausdrücklich vereinbarte Produktivfreigabe nicht für einen ausfallsicheren Dauerbetrieb vorgesehen.

2. **VM-Mitnutzung:** Der Kunde erhält projektabhängig Zugang zu einer virtuellen Maschine bzw. einer dort betriebenen Software-/Framework-Umgebung. Die Domain verweist auf die jeweilige Anwendung. Konkrete Ressourcen, Adminrechte, Updates, Monitoring, Erreichbarkeit und Verfügbarkeitsziele müssen bei Bedarf im Hauptvertrag geregelt werden; solche Zusagen entstehen nicht allein durch die AVV.

3. **Primäre Backup-Verantwortung des Kunden:** Soweit nicht schriftlich anders vereinbart, organisiert und überwacht der Kunde die fachlichen und anwendungsbezogenen Datensicherungen einschließlich Umfang, Häufigkeit, Ziel, Aufbewahrung, Zugang zu Backup-Konten, Löschfristen sowie regelmäßiger Wiederherstellungstests. Vor produktivem Einsatz muss er prüfen, ob die vereinbarte Backup-Lösung seinem Risiko entspricht.

4. **Unterstützung bei WordPress:** Der Auftragsverarbeiter kann auf Wunsch die Einrichtung geeigneter Plugins (etwa UpdraftPlus) unterstützen, z. B. zur Sicherung auf ein vom Kunden verwaltetes Google-Drive-Konto. Die Aktivierung eines Plugins oder ein einmaliger Funktionstest begründen keinen laufenden Sicherungs-/Kontrollauftrag. Google Drive kann ein weiterer datenschutzrechtlich relevanter Dienst sein; der Kunde prüft Rolle, Bedingungen und gegebenenfalls notwendige Verträge und Transfers.

5. **Freiwillige lokale Sicherungen:** Auf der eigenen Serverlandschaft können zusätzlich technische Snapshots oder lokale Datenkopien erstellt werden, soweit das jeweilige System dies vorsieht. Ohne separat dokumentierte Vereinbarung stellen sie keine zugesicherte, regelmäßig durchzuführende, vollständig verfügbare oder fristgerecht wiederherstellbare Backup-Dienstleistung dar. Der Kunde darf sich für seine Datensicherungsplanung nicht ausschließlich auf solche freiwilligen Kopien verlassen.

6. **Produktivsysteme:** Für Live-Websites und andere produktiv genutzte Anwendungen sind spätestens vor Produktivschaltung angemessene Sicherheits- und Backupmaßnahmen sowie Verantwortlichkeiten projektbezogen zu beurteilen und in Anlage 1 oder einer ergänzenden Betriebs-/Sicherungsvereinbarung festzulegen. Ohne solche Festlegung werden insbesondere kein Backup-Intervall, keine Wiederherstellungszeit (RTO), kein maximaler Datenverlustzeitraum (RPO) und keine garantierte Verfügbarkeit zugesichert. Unabdingbare Pflichten nach Art. 32 DSGVO bleiben davon unberührt.

7. **Haftungsabgrenzung:** Für das Unterbleiben kundenseitig übernommener oder ausdrücklich nicht beauftragter Backups wird keine vertragliche Erfolgs- oder Wiederherstellungsgarantie übernommen. Der Auftragsverarbeiter haftet jedoch nach den anwendbaren gesetzlichen und wirksam vereinbarten vertraglichen Regeln für Schäden aus eigener Pflichtverletzung; gesetzlich nicht ausschließbare Ansprüche, insbesondere nach Art. 82 DSGVO, bleiben unberührt.

§ 11 Vertragsende, Rückgabe, Löschung

Nach Ende der Beauftragung werden personenbezogene Daten nach Wahl des Kunden herausgegeben oder gelöscht, soweit keine Aufbewahrungspflichten entgegenstehen. Dabei sind auch vertraglich verwaltete Kopien zu berücksichtigen. Vorhandene technische Sicherungskopien werden nach dem dokumentierten Lösch-/Rotationsprozess entfernt und bis dahin geschützt. Rückgabe-/Exportleistungen und Fristen sind vor Beendigung abzustimmen; der Kunde sichert rechtzeitig seine erforderlichen Daten.

§ 12 Rangfolge und Schlussbestimmungen

Diese AVV ergänzt den Hauptvertrag und die AGB unter https://itlerhilfe.de/agb/. Bei datenschutzrechtlichen Widersprüchen haben zwingende DSGVO-Pflichten sowie die spezifischen Regelungen dieser AVV Vorrang. Leistungsumfang und Vergütung bestimmen sich im Übrigen nach dem Hauptvertrag. Änderungen und projektspezifische Anlagen bedürfen mindestens der Textform, soweit keine strengere gesetzliche Form vorgeschrieben ist.

Unterschriften

Kunde / Verantwortlicher: _____ Ort/Datum: _____

Unterschrift: _____

Ausgewählter Auftragsverarbeiter / Ing. Klaus Schlender: _____

Ort/Datum: _____ Unterschrift: _____

Anlage 1 – Projektbeschreibung und Betriebskonzept (auszufüllen)

Projekt / Domain / VM-Bezeichnung: _____

Leistung: ■ Software-Prototyp ■ WordPress ■ Entwicklung ■ Remote-Support ■ VM-Mitnutzung ■ Wartung ■ Sonstiges

Status: ■ Entwicklung/Test ■ Staging ■ Live/Produktion | Verantwortlich für Anwendungsbetrieb: _____

Betroffene: ■ Website-Besucher ■ Kunden ■ Beschäftigte ■ Benutzer ■ Sonstige: _____

Daten: ■ Kontaktdaten ■ Benutzerkonten ■ IP-/Logdaten ■ Inhalts-/Formulardaten ■ Sonstige: _____

Besondere Daten (Art. 9 DSGVO): ■ Nein ■ Ja – weitere Maßnahmen: _____

Auftragszweck / Verarbeitung: _____

Server: ■ VM in Espelkamp ■ Kunde/Externer Provider; Betriebssystem/Framework: _____

Zugriffe: ■ Kunde ■ Itlerhilfe OÜ ■ Quantum Solution ■ Dritte (Anlage 3); Länder: _____

Backup- und Wiederherstellungsvereinbarung:

Verantwortlich: ■ Kunde (Standard) ■ Auftragsverarbeiter (nur mit separater Leistungsabrede) ■ aufgeteilt: _____

Anwendungsbackup: ■ keines (nur zulässig nach Risikoprüfung) ■ Plugin ■ Skript ■ anderes: _____

Externer Speicherort: ■ kundenseitiges Google Drive ■ anderer: _____

Lokale technische Kopien: ■ nicht zugesichert ■ separat vereinbart: _____

Nur für vereinbarte Backups: Intervall _____; Aufbewahrung _____; RPO _____; RTO _____; Test _____

Verantwortung für Zugangsdaten, Zahlung und Kontrolle des Backup-Ziels: _____

Produktivfreigabe / individuelle Maßnahmen / Datenexport / Löschung: _____

Kontakt Sicherheitsvorfälle (Kunde): _____ Freigabe / Datum: _____

Anlage 2 – Technische und organisatorische Maßnahmen (TOM)

Prüfliste: Markierungen sind vor Vertragsabschluss anhand der tatsächlichen technischen Umsetzung zu bestätigen. Nicht angekreuzte Optionen gelten nicht automatisch als eingeführt. Technische Details können als vertrauliche Anlage beigefügt werden.

Zutritt / physische Sicherheit

■ Zutritt zum Serverbereich auf Berechtigte beschränkt; Schlüssel-/Raumsicherung dokumentiert

■ Schutz vor unbefugten Besuchern, Diebstahl und typischen Umgebungsrisiken

Zugang / Systemschutz

■ Rollen, individuelle Konten, Berechtigungsentzug und sichere Authentisierung

■ Abgesicherte Administrationszugänge, verschlüsselte Übertragung, MFA soweit passend

■ Patch- und Updateverfahren für vom Anbieter verwaltete Host-/Virtualisierungskomponenten

■ Netztrennung / Mandantentrennung zwischen VMs nach Schutzbedarf

■ Protokollierung relevanter Administrationszugriffe und Umgang mit Vorfällen

Entwicklung und Support

■ Trennung von Test- und Produktivdaten soweit möglich

■ Sicherer Umgang mit Schlüsseln, Secrets und Zugängen; Support-Rechte begrenzt

■ Vertraulichkeitsverpflichtung; Regeln für Fernarbeit / Homeoffice

Verfügbarkeit / Backup-Rollen

■ Risikoangemessene Host-/Infrastruktursicherungen und Wiederanlaufverfahren geprüft

■ Kunden-Backupverantwortung und mögliche lokale freiwillige Kopien dokumentiert

■ Bei Live-Betrieb: konkrete Datensicherung / Wiederherstellung nach Anlage 1 festgelegt

■ Speicherorte, Fristen und Zugriffsschutz tatsächlich vorhandener Sicherungen dokumentiert

Abweichungen und vorhandene Nachweise: _____

TOM geprüft am: _____ Durch: _____

Anlage 3 – Unterauftragsverarbeiter / externe Sicherungsziele

Genehmigung: ■ besondere Freigabe unten ■ allgemeine Freigabe nach § 7 einschließlich Änderungsmitteilung

■ Quantum Solution – Klaus Schlender; Entwicklung / Systemadministration in Deutschland, falls für Itlerhilfe OÜ mit Kundendaten tätig. ■ genehmigt ■ nicht eingesetzt

■ Itlerhilfe OÜ; Unterstützung / Entwicklung / Administration in Estland, falls für Quantum Solution mit Kundendaten tätig. ■ genehmigt ■ nicht eingesetzt

Weitere Unterauftragsverarbeiter (Name, Zweck, Sitz, Zugriff, Datenstandort, Genehmigung):

1. _____

2. _____

3. _____

Vom Kunden selbst eingesetzte Anbieter / Sicherungsziele (z.B. Google Drive mit UpdraftPlus; Einordnung prüfen):

_____

Zugriff/Datenübertragung außerhalb EU/EWR: ■ Nein ■ Ja, Land / Garantien: _____

Kundengenehmigung / Datum / Unterschrift: _____

Verwendungshinweis: Vor Unterschrift Geschäftsanschrift, Sicherheitsmaßnahmen, Unterauftragnehmer und projektspezifische Zuständigkeiten prüfen. Diese Vorlage ist keine individuelle Rechtsberatung.

Ergänzung zur AVV – Betriebsrisiken und Sicherungskonzept

Version 1.2 · 02.11.2026 · Bestandteil der AVV Version 1.1 zwischen dem auf Seite 1 ausgewählten Auftragsverarbeiter und dem Kunden.

Diese Ergänzung konkretisiert § 1 Abs. 2, § 4 sowie § 10 der beigefügten AVV. Bei Abweichungen gehen die nachstehenden Klarstellungen vor. Alle übrigen Regelungen und Anlagen der AVV bleiben bestehen.

1. Einordnung der Leistung / kein Managed Hosting

Die Mitnutzung der eigenen Serverlandschaft erfolgt insbesondere zur Entwicklung, Demonstration und zum Test von Prototypen sowie projektbezogen für virtuelle Maschinen mit kundenspezifischer Domain, Software oder Framework. Ohne gesonderten Vertrag sind weder ein vollumfängliches Managed Hosting noch eine Hochverfügbarkeitsleistung, 24/7-Überwachung, garantierte Reaktionszeit oder ein Service-Level-Agreement geschuldet. Für dauerhaft produktive und betreuungsintensive Internetangebote empfiehlt der Auftragsverarbeiter, ein gesondertes Hosting-Angebot eines spezialisierten Providers (z. B. STRATO oder eines vergleichbaren Anbieters) zu prüfen. Eine Wahl und Beauftragung eines solchen Providers trifft der Kunde selbst.

2. Infrastruktur-Backups und Kundendatensicherungen

Im Rahmen der eigenen Serververwaltung führt der Auftragsverarbeiter Sicherungen seiner Serverumgebung nach seinem internen Betriebskonzept durch. Diese können auch Kunden-VMs oder deren Daten erfassen. Solche Sicherungen dienen vorrangig dem eigenen Infrastrukturbetrieb und der Wiederherstellung im Rahmen der technisch vorhandenen Möglichkeiten. Sie sind ohne gesonderte schriftliche Vereinbarung keine garantierte, vollständige oder jederzeit abrufbare Sicherung individueller Kundendaten. Eine bestimmte Sicherungshäufigkeit, Aufbewahrungsfrist, Wiederherstellungszeit oder ein bestimmter Wiederherstellungspunkt ist damit nicht zugesagt. Tatsächlich vorhandene Sicherungskopien sind angemessen zu schützen.

3. Eigenverantwortung und Unterstützung des Kunden

Die Verantwortung für anwendungsbezogene Backups und deren Kontrolle liegt grundsätzlich beim Kunden, soweit nicht anders vereinbart. Bei WordPress kann der Auftragsverarbeiter etwa bei der Einrichtung von UpdraftPlus, bei lokalen Sicherungen und bei einer zusätzlichen Ablage in einem kundenseitig verwalteten Google-Drive-Konto unterstützen. Regelmäßige Überwachung, Wiederherstellungstests und eine fortlaufende Backup-Betreuung sind nur geschuldet, wenn sie ausdrücklich vereinbart werden. Für produktive Websites werden erforderliche Verfahren und Zuständigkeiten individuell vor der Produktivnutzung festgelegt.

4. Störungen, höhere Gewalt und Haftungsgrenzen

Stromausfall, Internet- oder Netzausfall, Brand, Einbruch, Diebstahl, Naturereignisse und sonstige Ereignisse außerhalb der zumutbaren Kontrolle des Auftragsverarbeiters können die Verfügbarkeit beeinträchtigen und zu Datenverlust führen. Soweit der Auftragsverarbeiter ein solches Ereignis und seine Folgen trotz der geschuldeten, angemessenen Sicherheitsvorkehrungen nicht zu vertreten hat, übernimmt er hierfür keine vertragliche Schadens- oder Verfügbarkeitsgarantie. Ein pauschaler Ausschluss für Schäden aus eigenem Vorsatz, grober Fahrlässigkeit, Verletzung wesentlicher Vertragspflichten oder zwingenden gesetzlichen Ansprüchen ist damit nicht verbunden. Ebenso bleiben die Pflichten aus Art. 28 und 32 DSGVO und mögliche Ansprüche nach Art. 82 DSGVO unberührt.

5. Erforderliche Einzelvereinbarung bei Live-Betrieb

Vor Produktivschaltung einer Website oder Anwendung dokumentieren die Parteien in Anlage 1 oder einem separaten Betriebsblatt mindestens: zuständige Person für Backup und Kontrolle, Sicherungsziel und -intervall, Aufbewahrung, etwaige Wiederherstellungsziele sowie vereinbarte Sicherheits- und Verfügbarkeitsmaßnahmen. Ohne solche Vereinbarung entstehen keine zusätzlichen Leistungszusagen; rechtlich erforderliche Schutzmaßnahmen bleiben gleichwohl geschuldet.

Auftraggeber (Kunde): _____ Datum: _____

Unterschrift Kunde: _____ Unterschrift Auftragnehmer: _____

Ergänzung zur AVV – STRATO-VPS als öffentlicher Netzwerkzugang

Version 1.3 · 02.11.2026 · Diese Ergänzung ist zusammen mit der beigefügten AVV Version 1.1 und der Betriebsrisiken-Ergänzung Version 1.2 zu verwenden. Sie gilt für den auf Seite 1 ausgewählten Vertragspartner und dessen Kunden.

1. Technischer Datenweg

Der Auftragnehmer betreibt einen virtuellen Server (VPS) bei STRATO als vorgeschalteten öffentlichen Netzwerk-Endpunkt mit öffentlicher IP-Adresse. Eingehende Verbindungen zu den bereitgestellten Kundenanwendungen werden über diesen VPS an die eigene Firewall des Auftragnehmers und von dort an dessen Serverinfrastruktur am Standort Graudenzer Weg 10, 32339 Espelkamp, Deutschland weitergeleitet. Dort befinden sich die kundenseitig genutzten virtuellen Maschinen (VM), Anwendungen, WordPress-Installationen und Datenbanken, soweit im Hauptvertrag nichts Abweichendes festgelegt ist.

2. Zweck und mögliche Datenverarbeitung

Der STRATO-VPS dient der öffentlichen Erreichbarkeit und Weiterleitung des Netzwerkverkehrs, nicht als regulärer Speicherort für Kunden-Websites, Anwendungsdatenbanken oder deren anwendungsbezogene Backups. Bei Verbindungen können insbesondere IP-Adressen, Port- und Verbindungsinformationen, Zeitstempel sowie abhängig von der konkreten technischen Konfiguration Log- und weitere Verkehrsdaten verarbeitet werden. Ob Inhalte oder TLS-/HTTPS-Nutzdaten auf dem VPS entschlüsselt oder zwischengespeichert werden, ist vor Freigabe der jeweiligen Konfiguration zu dokumentieren. Aus der bloßen Weiterleitung folgt keine Zusage einer Ende-zu-Ende-Verschlüsselung.

3. Einordnung von STRATO und Unterauftragsverarbeitung

Soweit STRATO im Rahmen des VPS-Betriebs personenbezogene Daten im Auftrag des gewählten Auftragsverarbeiters verarbeitet, wird STRATO als Unterauftragsverarbeiter gemäß § 7 und Anlage 3 der AVV eingesetzt. Vor dem entsprechenden Einsatz sind die erforderliche Kundengenehmigung und eine geeignete Vereinbarung mit STRATO nach Art. 28 DSGVO sicherzustellen. Die rechtliche Einordnung richtet sich nach den tatsächlich erbrachten Leistungen und vertraglichen Rollen; reine Telekommunikationsübermittlung ist nicht pauschal einer Auftragsverarbeitung gleichzusetzen.

4. Technische und organisatorische Maßnahmen

Die Weiterleitung über STRATO ist Bestandteil der in Anlage 2 beschriebenen Netzinfrastruktur. Der Auftragnehmer dokumentiert und prüft risikobasiert die eingesetzten Schutzmechanismen (z. B. abgesicherter Transport zur eigenen Firewall, Firewall-Regeln, administrativer Zugriff, Patchmanagement und erforderliche Protokollierung), soweit sie tatsächlich implementiert sind. Ein Ausfall des STRATO-VPS, seiner Netzanbindung oder des Weiterleitungswegs kann die Erreichbarkeit der Kunden-VM beeinträchtigen; eine gesonderte Hochverfügbarkeits- oder Managed-Hosting-Zusage entsteht hierdurch nicht.

5. Verhältnis zu den übrigen Regelungen

Die Regelungen zu Prototypen, optionaler VM-Mitnutzung, kundenverantworteten Anwendungsbackups, freiwilligen Infrastruktursicherungen, Live-Betrieb und Haftungsgrenzen aus der AVV und Ergänzung Version 1.2 gelten unverändert. Gesetzlich zwingende Datenschutz- und Sicherheitsverpflichtungen sowie nicht abdingbare Haftung bleiben unberührt. Bei Widersprüchen hinsichtlich des Netzwerkzugangs geht diese Ergänzung vor.

Ergänzung zu Anlage 3 – Unterauftragsverarbeiter

STRATO GmbH · Rolle: Anbieter eines vorgeschalteten VPS/öffentlichen Netzwerkzugangs; Leistung: Weiterleitung eingehender Verbindungen zur kundengenutzten Infrastruktur in Espelkamp; mögliche Daten: IP- und Verbindungsdaten, gegebenenfalls technische Logs sowie weitere Daten entsprechend der realen Konfiguration. Freigabe durch den Kunden: ☐ genehmigt ☐ nicht eingesetzt / gesondert zu prüfen. TLS-/Weiterleitungsart: ☐ reine Weiterleitung ohne TLS-Terminierung ☐ TLS-Terminierung auf VPS ☐ andere: _____.

Kunde / Auftraggeber: _____ Ort / Datum: _____

Unterschrift Kunde: _____ Unterschrift Auftragnehmer: _____

Hinweis: Konfiguration, tatsächlicher STRATO-Vertrag und Anlagen sind vor Unterzeichnung zu verifizieren. Diese Vorlage ersetzt keine individuelle anwaltliche Prüfung.