Auftragsverarbeitungsvertrag (AVV)

Inhaltsverzeichnis

KONTAKT

imos Gesellschaft für Internet-Marketing und Online-Services mbH | Alfons-Feifel-Str. 9 | 73037 Göppingen

Telefon: 07161 93339-0 | Telefax: 07161 93339-99
E-Mail: info@imos.net | Internet: www.imos.net

GESCHÄFTSFÜHRUNG

Alfred Wallender
Rolf Wallender

Amtsgericht Ulm | HRB 532571
USt-IdNr.: DE182917076

BANKVERBINDUNG

Kreissparkasse Göppingen | GOPSDE6GXXX
IBAN: DE44 6105 0000 0049 0644 23

Volksbank Göppingen | GENODES1VGP
IBAN: DE85 6106 0500 0436 2640 05

1 Präambel

Dieser Auftragsverarbeitungsvertrag (nachfolgend „Auftrag“) regelt die Verpflichtungen zwischen der imos Gesellschaft für Internet-Marketing und Online-Services (nachfolgend „Auftragnehmer“) und dem Auftraggeber gemäß Punkt 18.1 im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag. Dieser Auftrag findet Anwendung auf alle Tätigkeiten, die mit dem Dienstleistungsvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer Beauftragte („Unterauftragnehmer“) personenbezogene Daten („Daten“) des Auftraggebers verarbeiten. In diesem Auftragsverarbeitungsvertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutzgrundverordnung (DSGVO) zu verstehen.

2 Gegenstand des Auftrags

Der Auftrag gilt für nachfolgende Leistungen:

- Bereitstellung und Überlassung von Webhosting.
- Bereitstellung und Überlassung von E-Mail inkl. Spam- und Virenfilter.
- Entwicklung und Betrieb von Webseiten und webbasierten Anwendungen.

3 Dauer

Die Laufzeit des Auftragsverarbeitungsvertrags richtet sich nach dem Zeitraum der jeweiligen Leistungserbringung. Dieser ergibt sich aus einem separaten Vertrag über die Nutzung der Dienste des Auftragnehmers durch den Auftraggeber.

Beide Parteien können den Auftrag mit einer Frist von drei Monaten zum Quartalsende kündigen, wobei das Recht zur fristlosen Kündigung unberührt bleibt. Eine Kündigung des Auftrags führt nicht automatisch zur Beendigung der entsprechenden Dienste.

Während der Dauer der Leistungserbringung sind die Vertragspartner gesetzlich verpflichtet, einen gültigen Auftragsverarbeitungsvertrag aufrechtzuerhalten. Im Falle einer Kündigung des Auftrags müssen die Vertragspartner diesen durch einen neuen, gültigen Auftragsverarbeitungsvertrag ersetzen.

Sofern im Hauptvertrag nichts anderes geregelt ist, bedarf jede Kündigung der Schriftform.

4 Art und Zweck der Verarbeitung

Der Auftragnehmer erbringt, gemäß den Anweisungen des Auftraggebers, bzw. die sich aus der Leistungsvereinbarung ergebenden Dienstleistungen, wie Wartung, Pflege und Support für die beim Auftraggeber eingesetzten IT-Produkte des Auftragnehmers.

5 Art der personenbezogenen Daten und Kategorien betroffener Personen

Die Art der personenbezogenen Daten und die Kategorien betroffener Personen, die Gegenstand dieses Auftrages sind, werden in Anlage 1 definiert.

6 Technische und organisatorische Maßnahmen

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 die Dokumentation zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung des Auftraggebers einen Anpassungsbedarf erfordert, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c) und Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und zu gewährleisten. Insgesamt handelt es sich bei den dabei zu treffenden technischen und organisatorischen 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.

Die Einzelheiten der technischen und organisatorischen Maßnahmen des Auftragnehmers sind in der Anlage 2 beschrieben.

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.

Wenn der Auftraggeber nach Abschluss dieses Auftrages entscheidet, dass die bislang vorhandenen technischen und organisatorischen Maßnahmen des Auftragnehmers zum Schutz bestimmter personenbezogener Daten unter Berücksichtigung der Kriterien des Art. 32 Abs. 1 DSGVO nicht ausreichen, wird er dem Auftragnehmer die zusätzlich erforderlichen Maßnahmen benennen und mit dem Auftragnehmer eine Vereinbarung treffen, wer welche Maßnahmen zu welchen Kosten veranlassen wird.

7 Ort der Verarbeitung

Die Verarbeitung der Daten findet in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

Jede Verlagerung der Daten in einen anderen Staat (sogenanntes „Drittland“) bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

8 Weisungsbefugnis des Auftraggebers

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur im Rahmen der getroffenen Vereinbarungen bzw. nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften (Art. 28 Abs. 3 S. 3 DSGVO).

9 Rechte und Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags auch gegenüber dem Auftraggeber die gesetzlichen Pflichten gemäß den Art. 28 bis 33 DSGVO zu erfüllen. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben und ist zu folgenden Maßnahmen verpflichtet:

- Die Wahrung der Vertraulichkeit gemäß den 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 Auftrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß den Art. 28 Abs. 3 S. 2 lit. c), 32 DSGVO. Die Einzelheiten sind in Anlage 2 dieses Auftragsverarbeitungsvertrags beschrieben.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Der Auftragnehmer verpflichtet sich, den Auftraggeber im erforderlichen Umfang zu unterstützen, sofern der Auftraggeber im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer einer Kontrolle durch eine zuständige Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, der Geltendmachung von Haftungs- oder Schadensersatzansprüchen durch eine betroffene Person oder einen Dritten oder sonstigen Ansprüchen ausgesetzt ist.
- 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.

- Der Auftragnehmer weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber nach Ziffer 11 dieses Auftrages und die Erledigung aller Pflichten gemäß Ziffer 9 dieses Auftrages nach.

10 Unterauftragsverhältnisse

Hinsichtlich der Beauftragung von Unterauftragnehmern vereinbaren die Parteien Folgendes:

☐ Der Auftragnehmer darf Unterauftragsverhältnisse hinsichtlich der vertragsgegenständlichen Verarbeitung personenbezogener Daten nur nach vorheriger schriftlicher Zustimmung des Auftraggebers begründen (gemäß Art. 28 Abs. 2 S. 1 DSGVO).

☒ Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, Unterauftragnehmer einzusetzen. Der Auftragsverarbeiter informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (gemäß Art. 28 Abs. 2 S. 2 DSGVO). Der Einspruch ist innerhalb von 4 Wochen geltend schriftlich oder in Textform zu machen. Ein Einspruch ist nur aus wichtigem Grund möglich und die wichtigen Gründe sind mitzuteilen. Im Fall eines fristgerechten Einspruchs kann der Auftragnehmer nach eigener Wahl entweder seine Leistungen ohne Hinzuziehung des Unterbeauftragten fortsetzen oder das Vertragsverhältnis mit dem Auftraggeber (einschließlich eines etwaig bestehenden Hauptvertrags) innerhalb einer Frist von 4 Wochen kündigen. Sofern die Leistungen des Auftragnehmers teilbar sind und sich der betreffende Unterauftrag lediglich auf einen bestimmten Leistungsteil bezieht, ist auch eine Teilkündigung durch den Auftragnehmer zulässig.

- Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- Der Auftragnehmer hat den Unterauftragnehmer schriftlich in gleichem Umfang zu verpflichten, wie er selbst aufgrund dieses Auftrages gegenüber dem Auftraggeber verpflichtet ist.
- Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers gemäß Art. 28 Abs. 4 DSGVO.
- Der Auftragnehmer wird sich vor Beauftragung von der Einhaltung der beim Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen.
- Sofern eine Einbeziehung von Unterauftragnehmern in Drittländern erfolgen soll, stellt der Auftragnehmer sicher, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau im Sinne der Art. 44 ff. DSGVO gewährleistet ist. Der Unterauftragnehmer hat einen Vertreter in der EU zu bestellen.
- Der Auftraggeber stimmt hiermit der Begründung der Unterauftragsverhältnisse gemäß Anlage 3 zu.

11 Kontrollrechte des Auftraggebers

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann.

Der Auftragnehmer wird im Rahmen der Prüfung alle erforderlichen Informationen und Auskünfte erteilen, Unterlagen vorlegen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachweisen.

Der Auftraggeber darf nach rechtzeitiger Abstimmung, zu den üblichen Geschäftszeiten, die technischen und organisatorischen Maßnahmen des Auftragnehmers zur Einhaltung dieses Auftrages prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

12 Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten zum Schutz personenbezogener Daten. Hierzu gehören unter anderem:

- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- 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,
- die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgenabschätzung,
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Nach der Meldung einer Verletzung personenbezogener Daten durch den Auftragnehmer an den Auftraggeber entscheidet der Auftraggeber in alleiniger Verantwortung, ob die Voraussetzungen für eine Meldung an Behörden bzw. betroffene Personen vorliegen, und nimmt die Meldungen in alleiniger Verantwortung vor.

13 Löschung und Rückgabe von personenbezogenen Daten

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. Die gesetzlichen Aufbewahrungspflichten bleiben unberührt.

14 Haftung

Es gelten die gesetzlichen Haftungsregelungen gemäß Art. 82 DSGVO. Etwaige Haftungsbegrenzungen zwischen den Parteien (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung.

15 Vergütung für Unterstützungsleistungen

Für Unterstützungsleistungen gemäß diesem Auftrag, die nicht von bestehenden Leistungsvereinbarungen (Hauptvertrag; Rahmenvertrag; Vergütungsvereinbarung) und der dort geregelten Vergütung erfasst sind, kann der Auftragnehmer zu den aktuell geltenden Preisen eine Vergütung verlangen. Ebenso kann er für den Ihm entstandenen Aufwand nach den jeweiligen gesetzlichen Voraussetzungen eine entsprechende Entschädigung verlangen.

Dies gilt nicht, sofern die Leistungen auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind.

Etwaige entstehende Kosten müssen verhältnismäßig sein, sind vom Auftragnehmer vorab anzukündigen und mit dem Auftraggeber abzustimmen.

16 Schlussbestimmungen

Für diesen Auftrag gilt deutsches Recht. Sollte eine Vertragsbestimmung unwirksam sein oder werden, so berührt dies die Gültigkeit des übrigen Auftragsinhalts nicht. Die o.g. Parteien werden sich bemühen, in einem solchen Fall, eine in ihrem wirtschaftlichen Ergebnis dem jetzigen Sinn entsprechende Lösung zu finden. Dies gilt auch, wenn bei Durchführung des Auftrags eine ergänzungsbedürftige Lücke offenbart wird.

Änderungen und Ergänzungen dieses Auftrages bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

17 Anlagen

Anlagen zu diesem Auftrag sind:

- Anlage 1 – Kategorien personenbezogenen Daten und betroffener Personen
- Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers
- Anlage 3 – Unterauftragnehmer
- Anlage 4 – Technische und organisatorische Maßnahmen im EVF-Datacenter (Auszug)

18 Vertragsparteien/Unterschriften

18.1 Auftraggeber/Verantwortlicher

Kundennummer	
Firma/Name	
Strasse	
PLZ, Ort	
Land	Deutschland
Registergericht	
Vertreten durch	
Datum, Unterschrift	

18.2 Auftragnehmer/Auftragsverarbeiter

Firma	imos Gesellschaft für Internet-Marketing und Online-Service mbH
Strasse	Alfons-Feifel-Str. 9
PLZ, Ort	73037 Göppingen
Land	Deutschland
Vertreten durch	Alfred oder Rolf Wallender
Datum, Unterschrift	

Anlage 1 – Kategorien personenbezogener Daten und betroffener Personen

1 Kategorie der personenbezogenen Daten

Folgende Kategorien von Daten sind Gegenstand dieses Auftrags:

- ☒ Stammdaten (z.B. Vorname, Name, Bankverbindung)
- ☒ Kontaktdaten (z.B. Anschrift, Rufnummern, E-Mailadresse)
- ☒ Kommunikationsdaten (z.B. E-Mails, Tickets)
- ☒ Inhaltsdaten der gebuchten Dienste des Auftraggebers (z.B. Bestellungen, Verträge)
- ☒ Verkehrsdaten (z.B. Quell-/Zielkennung, IP-Adresse, Zeitstempel)

2 Kategorien betroffener Personen

Folgende Kategorien von Betroffenen sind Gegenstand des Auftrags:

- ☒ Interessenten des Auftraggebers
- ☒ Kunden des Auftraggebers
- ☒ Lieferanten des Auftraggebers
- ☒ Mitarbeiter des Auftraggebers
- ☒ Nutzer der gebuchten Dienste des Auftraggebers

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anforderungsbeschreibung:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

1.1 Pseudonymisierung

- Sofern technisch möglich und sinnvoll, werden vom Auftragnehmer vergebene Benutzerkennungen und Verzeichnisse auf Dateisystemen pseudonymisiert.

1.2 Verschlüsselung

- Der Datenverkehr zwischen Mail-Servern wird standardmäßig per SSL/TLS angeboten. Damit auch ältere Mail-Server eine Verbindung herstellen können, besteht alternativ die Möglichkeit einer unverschlüsselten Verbindung.
- Der Datenverkehr zwischen Mail-Client und Mail-Server wird standardmäßig per SSL/TLS angeboten. Auch hier wird bei älteren Clients die Verbindung ohne Verschlüsselung ermöglicht.
- Für Webspace und Webhosting wird die Datenübertragung über SFTP bzw. FTPS sichergestellt.
- Für Webspace und Webhosting ist HTTPS möglich, die Aktivierung obliegt dem Kunden.
- Vom Auftragnehmer erstellte Webseiten werden über das Protokoll HTTPS bereitgestellt.

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

2.1 Zutrittskontrolle

- Alle für diesen Auftrag eingesetzten Server werden im EVF-Datacenter, Göppingen betrieben. Die technischen und organisatorische Maßnahmen werden in Anlage 4 beschrieben.

2.2 Zugangskontrolle

- Fernzugriffe auf interne Systeme werden durch Firewalls geschützt.
- Fernzugriff auf das interne Netzwerk erfolgt ausschließlich per VPN.
- Wo technisch möglich, wird eine 2-Faktor-Authentifizierung eingesetzt.
- Sofern technisch sinnvoll, werden Systeme durch aktuelle Virenschutzmaßnahmen abgesichert.
- Zugangsdaten zu internen Systemen werden verschlüsselt übertragen.
- Der Zugang zum Backend wird kontrolliert und sämtliche Zugriffe protokolliert.

2.3 Zugriffskontrolle

- Der Zugriff auf personenbezogene Daten erfolgt ausschließlich in authentifizierter Form.
- Ein festgelegtes Rollen- und Rechtekonzept regelt den Datenzugriff.
- Kritische Systeme sind ausschließlich für ausgewählte Administratoren zugänglich.

2.4 Trennungskontrolle

- Entwicklungs-, Produktions- und Testumgebungen werden virtuell getrennt.
- Die Datensätze werden durch ein Mandantenkonzept voneinander getrennt.
- Eine Trennung der Daten nach Verwendungszweck wird gewährleistet.

2.5 Homeoffice

- Es wird ausschließlich aktuelle Hard- und Software für Arbeitsplatzgeräte eingesetzt.
- Eine private Nutzung betrieblicher Hardware ist untersagt.
- Arbeitsplatzgeräte werden durch Kennwort- oder biometrische Authentifizierung vor unbefugtem Zugriff geschützt.
- Der Zugriff auf die Serverinfrastruktur erfolgt ausschließlich über gesicherte und verschlüsselte VPN-Verbindungen.
- Beim Verlassen des Arbeitsplatzes werden die Arbeitsplatzgeräte stets gesperrt.
- Die Clean-Desk-Policy wird konsequent umgesetzt.
- Support-Zugriffe auf personenbezogene Daten erfolgen ausschließlich durch datenschutz-geschultes und -sensibilisiertes Personal.
- Eine lokale Datenhaltung sowie die Verarbeitung von Daten in Anwesenheit Dritter werden unterbunden.

3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

- Es werden Zugriffskontrollen implementiert, um sicherzustellen, dass nur autorisierte Personen auf personenbezogene Daten zugreifen können.
- Vor der Weitergabe von personenbezogenen Daten erfolgt stets eine Überprüfung der Identität und Autorisierung der Empfänger.
- Durch den Einsatz moderner Verschlüsselungstechnologien wird die Integrität und Vertraulichkeit der Daten während der Übertragung gewährleistet.

3.2 Eingabekontrolle

- Sofern die Datenintegrität nicht bereits durch eine Datenbank sichergestellt werden kann, erfolgen stichprobenartige Kontrollen, ob die eingegebenen Daten dem vorgesehenen Format entsprechen (z.B. bei Straßennamen und Hausnummern).
- Sofern die Plausibilität nicht bereits durch eine Datenbank sichergestellt werden kann, erfolgen stichprobenartige Kontrolle, ob die eingegebenen Werte in einem plausiblen Bereich liegen (z.B. Alter zwischen 1 und 120 Jahren).
- Sofern die Datenvalidierung nicht bereits durch eine Datenbank sichergestellt werden kann, erfolgen stichprobenartige Kontrollen, ob die eingegebenen Daten den gesetzlichen oder internen Vorgaben entsprechen (z.B. Prüfung der IBAN-Nummer).
- Es wird sichergestellt, dass nur autorisierte Personen Daten eingeben, ändern oder löschen dürfen.
- Sofern technisch möglich und sinnvoll, erfolgt die Protokollierung über die Erfassung und Speicherung von Informationen.

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

4.1 Verfügbarkeitskontrolle

- Die technischen und organisatorische Maßnahmen im EVF-Datacenter werden in Anlage 4 beschrieben.
- Die Serverhardware ist mehrfach redundant und ausfallsicher konzipiert.
- Zentrale Dienste werden kontinuierlich durch ein Monitoring überwacht.
- Updates und Patches werden zeitnah eingespielt.

- Daten werden regelmäßig gesichert und Backups werden erstellt, die an räumlich getrennten Standorten aufbewahrt werden.
- Virenschutz, Firewalls und weitere sicherheitsrelevante Systeme werden stets auf dem aktuellen Stand gehalten.

5 Wiederherstellbarkeit der Verfügbarkeit und des Zugangs (Art. 32 Abs. 1 lit. c DSGVO)

5.1 Rasche Wiederherstellbarkeit

- Es werden regelmäßige Sicherungskopien (Backups) erstellt, um im Falle eines Verlusts oder einer Beschädigung die zeitnahe Wiederherstellung aller Daten zu ermöglichen.
- Es gibt einen Notfallwiederherstellungsplan, der sicherstellt, dass Daten nach einem Vorfall schnell und effektiv wiederhergestellt werden können.
- Während eines Wiederherstellungsprozesses wird die Integrität der Daten gewährleistet, um sicherzustellen, dass Daten während der Wiederherstellung nicht beschädigt oder verändert werden.
- Der Zugriff auf wiederhergestellte Daten wird streng kontrolliert, um unbefugten Zugriff zu verhindern und sicherzustellen, dass nur autorisierte Personen Zugang haben.

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

6.1 Überprüfung

- Die technischen und organisatorische Maßnahmen im EVF-Datacenter werden in Anlage 4 beschrieben.
- Die Wirksamkeit der technischen Schutzmaßnahmen wird mindestens einmal jährlich überprüft.
- Regelmäßige Schulungen aller Mitarbeiter, die mit personenbezogenen Daten arbeiten, stellen die Einhaltung der gesetzlichen Vorschriften sicher.
- Datenschutzfreundliche Voreinstellungen unserer Dienste tragen zur Minimierung personenbezogener Daten bei.
- Subunternehmer und Auftragsverarbeiter werden sorgfältig ausgewählt. Es werden entsprechende Verträge abgeschlossen, deren Einhaltung regelmäßig überprüft wird.
- Datenschutzvorfälle werden umgehend dokumentiert und ausgewertet.
- Durch regelmäßige Sicherheitsaudits wird die Wirksamkeit der technischen und organisatorischen Maßnahmen überprüft.
- Eine Datenschutz-Folgenabschätzung (DPIA) erfolgt regelmäßig zur Bewertung datenschutzrelevanter Risiken.

6.2 Auftragskontrolle

- Es wird sichergestellt, dass der Auftragnehmer einen geeigneten Vertrag zur Auftragsverarbeitung abschließt.
- Es erfolgt eine Überprüfung, ob der Auftragnehmer die erforderlichen technischen und organisatorischen Maßnahmen (z.B. Verschlüsselung, Zugriffskontrollen, Datensicherung) umsetzt.
- Es wird kontrolliert, dass personenbezogene Daten ausschließlich auf ausdrückliche Anweisung des Verantwortlichen verarbeitet werden.

Anlage 3 – Unterauftragnehmer

Name	Anschrift	Leistung	Kommentar
FP Digital Business Solutions GmbH	Griesbergstr. 8 31162 Bad Salzdetfurth Deutschland	Signaturlösung „FP Sign“ zur digitalen Unterzeichnung von Verträgen	Die Serverstandorte befinden sich in Deutschland
LINET Services GmbH	Hinter dem Turme 12a 38114 Braunschweig Deutschland	Betreuung Microsoft-Server	Die Server werden vom Auftragnehmer selbst betrieben. Die Serverstandorte befinden sich in Deutschland
Microsoft Corporation	One Microsoft Way Redmond, WA 98052-6399 USA	Microsoft 365-Dienste, wie Microsoft Teams, OneDrive und SharePoint Online	Die Serverstandorte befinden sich in Europa
Microsoft Ireland Operations Limited	One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Ireland	Microsoft 365-Dienste, wie Microsoft Teams, OneDrive und SharePoint Online	Die Serverstandorte befinden sich in Europa
MWC - Mobile World Communications GmbH	Kavalierstr. 9 13187 Berlin Deutschland	Sekretariatsdienstleistungen (Anrufannahme)	Die Serverstandorte befinden sich in Europa
Znuny GmbH	Marienstraße 11 10117 Berlin Deutschland	Betreuung Ticketsystem Znuny (ehm. OTRS)	Die Server werden vom Auftragnehmer selbst betrieben. Die Serverstandorte befinden sich in Deutschland

Anlage 4 – Technische und organisatorische Maßnahmen im EVF-Datacenter (Auszug)

Alle für diesen Auftrag eingesetzten Server werden im Rechenzentrum der EVF in Göppingen, Deutschland betrieben. Das EVF-Datacenter ist nach DIN EN 50600 und ISO/IEC 27001 zertifiziert. Nachfolgend werden die relevanten technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO aufgeführt. Eine vollständige Übersicht des Sicherheitskonzepts erhalten Sie auf Nachfrage.

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

1.1 Zutrittskontrolle

- Zutritt ausschließlich für zutrittsberechtigte Personen.
- Zutritt für Dritte ausschließlich in Begleitung zutrittsberechtigter Personen.
- Zutrittskontrolle mit 2-Faktor-Authentifizierung, mehrstufig mit Biometrie.
- Zutritte werden protokolliert.

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

2.1 Gebäudeschutz

- Das Gelände wird durch einen Stabgitterzaun mit Übersteigschutz gesichert.
- Bauweise des Gebäudes in Stahlbeton.
- Das Gebäude ist mit Sicherheitstüren ausgestattet (feuerhemmend, rauchgasdicht und je nach Schutzzone in der Widerstandsklasse 2 bis 4 ausgeführt).
- Es sind keine Fenster vorhanden.
- Eine Einbruchmeldeanlage sowie ein alarmgesichertes Gebäudekonzept sind implementiert.
- Alarmmeldungen werden rund um die Uhr an eine Leitwarte weitergeleitet.
- Eine Videoüberwachung mit Aufzeichnung ist installiert.
- Überwachung und Störungsannahme durch Leitstelle (24/7).
- Störungsbeseitigung und Remote-Hands durch Notfallmanager (24/7).
- Glaselemente durchwurfhemmend und mit Sensoren gesichert.
- Personenschleuse aus Stahl-Glas-Konstruktion mit einbruchhemmendem Panzerglas.

2.2 Verfügbarkeit

- Die Zuführung aller Leitungswege erfolgt unterirdisch.
- Redundante Mittelspannungszuleitungen.
- Redundante Transformatoren.
- Netzersatzanlage (NEA) und Tankbevorratung.
- Unterbrechungsfreie Stromversorgung (USV).
- Redundante und räumlich getrennte Stromverteilungen.
- Unterverteilungen mit getrennten Stromkreisen.
- Differenzstrommessung Typ B an den PDUs.
- Redundante Klimatisierungsanlagen zur konstanten Kühlung der Racks.
- Mehrere Anfahrtswege über öffentliche Straßen.
- Der Betreiber des Datacenters bildet zugleich das Versorgungsunternehmen für die Energieversorgung und den Energienetzbetreiber.
- Versorgung über weiteres Umspannwerk möglich.

2.3 Belastbarkeit

- Das Gelände liegt ca. 360 m ü. NN (EFH).
- Keine geotechnischen Gefährdungen zu erwarten (lt. geotechnisches Gutachten und Kernbohrungen) .
- Erdbebenzone 0. Nicht-Überschreitungswahrscheinlichkeit von 90% der Intensität von < 6,5 (EMS-Skala) innerhalb von 50 Jahren lt. Innenministerium des Landes Baden-Württemberg.
- Keine Flüsse oder Seen im Umfeld.
- Abschüssiges Terrain um das Gebäude des EVF-Datacenters.
- Kein Hochwasserrisiko lt. Hochwasserrisikobewertung des Ministeriums für Umwelt, Klima und Energiewirtschaft Baden-Württemberg.
- Kein speziell ausgewiesenes Überflutungsgebiet.
- Überwachung Wasserleckage im Gefahrenbereich.
- Keine Waldbrände zu erwarten und im Umfeld nicht bekannt.
- Abgestimmtes Blitz- und Überspannungsschutzkonzept in Blitzschutzklasse 1.
- Die Erdungs- und Potentialausgleichsanlage als Schutz vor Blitzschlag und elektromagnetischen Beeinflussungen ist in das Fundamentsystem integriert.
- Separate Brandabschnitte.
- Stahlbetonwände und Türen der Sicherungsbereiche mindestens in F90.
- Brandfrüherkennung durch Ansaugrauchmeldesystem inkl. automatische Alarmierung der Feuerwehr.
- Automatische Stickstoff-Löschanlage.
- Keine elektromagnetische Beeinflussung wie Hochspannungsleitungen oder Sendestationen bekannt.
- Keine Luftverunreinigungen durch natürliche Ursachen zu erwarten.
- Keine ungewöhnlich hohen Windgeschwindigkeiten zu erwarten.
- Dampfdichte Ausführung insbesondere der Böden und Dächer (Bauausführung als „weiße Wanne“).
- Weitere Schutzmaßnahmen vor Elementargefährdungen führen zu einer Reduzierung von Brandlasten im Umfeld und innerhalb des Datacenters.
- Keine Orte von öffentlichem Interesse, Versammlungsorte oder potenziell politische Ziele bekannt.
- Keine Gewerbeimmobilien mit sicherheitsrelevanten Gefahren wie Lagerung/Verarbeitung von nuklearen, toxischen, explosiven oder entflammbaren Stoffen angrenzend.
- Keine hohen oder instabilen Anlagen im Umfeld.
- Keine Schwingungsquellen wie Hammerwerke oder Gleisanlagen im Umfeld.
- Schwingungsentkopplung der Rack-Aufbauten durch PUR Elastomer (Sylomer).
- Kein Schienenverkehr und i.d.R. kein Gefahrenstofftransport.
- Keine Bundesautobahnen, Bundesstraßen, Landesstraßen oder Kreisstraßen im Umfeld.
- Nicht im Bereich der üblichen An- oder Abflugrouten (Flughafen Stuttgart 34 km Luftlinie entfernt).

3 Wiederherstellbarkeit der Verfügbarkeit und des Zugangs (Art. 32 Abs. 1 lit. c DSGVO)

- Monitoring (24/7).
- Notfall-Hotline (24/7).
- Notfallpläne für Störungsfälle.

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

- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens einmal jährlich durchgeführt.
- Abschluss notwendiger Vereinbarungen mit eventuellen Subunternehmern/Auftragsverarbeitern und deren Überprüfung.