Vertrag zur Auftragsverarbeitung.

zwischen:

Auftraggeber:
Straße:
Ort:

nachfolgend Auftraggeber genannt und

snapAddy GmbH
Haugerkirchgasse 7
97070 Würzburg

nachfolgend Auftragnehmer genannt

§ 1 Gegenstand und Dauer des Auftrags

1. Der Auftragnehmer erbringt für den Auftraggeber die in Anhang 1 beschriebenen Leistungen im Rahmen der Auftragsverarbeitung. Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen ergeben sich abschließen aus Anhang 1.
2. Dieser Vertrag ist akzessorisch zum jeweils zugrunde liegenden Hauptvertrag zwischen den Parteien und tritt mit dessen Wirksamwerden in Kraft.
3. Der Vertrag gilt für die Dauer der Erbringung der vertraglich vereinbarten Leistungen sowie darüber hinaus, solange der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Mit Beendigung der Verarbeitungstätigkeit enden die Pflichten aus diesem Vertrag unbeschadet etwaiger gesetzlicher Aufbewahrungspflichten.

§ 2 Weisungen des Auftraggebers

1. Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Vorschriften, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich.
2. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, soweit er nicht durch das Recht der Europäischen Union oder der Mitgliedsstaaten zur Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.
3. Weisungen sind grundsätzlich in Textform zu erteilen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Alle erteilten Weisungen sind vom Auftraggeber und Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für einen Zeitraum von drei (3) weiteren Jahren aufzubewahren, sofern im Einzelfall keine längere gesetzliche Aufbewahrungspflicht besteht.

4. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.
5. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Änderung der Leistung behandelt und können vom Auftragnehmer von einer angemessenen Vergütung abhängig gemacht werden.

§ 3 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer verpflichtet sich, geeignete technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO zu ergreifen und dauerhaft aufrechtzuerhalten. Diese Maßnahmen berücksichtigen den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.
2. Die konkret umgesetzten technischen und organisatorischen Maßnahmen sind in Anhang 3 beschrieben. Sie gewährleisten ein dem Risiko angemessenes Schutzniveau. Ein Anspruch auf eine bestimmte technische Ausgestaltung besteht nicht.
3. Der Auftragnehmer ist verpflichtet, die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und bei Bedarf anzupassen, insbesondere bei technischen Weiterentwicklungen oder veränderten Risiken.
4. Anpassungen der technischen und organisatorischen Maßnahmen dürfen vorgenommen werden, sofern das Schutzniveau dadurch nicht unterschritten wird. Wesentliche Änderungen, die das Schutzniveau oder die Art der Verarbeitung betreffen können, sind dem Auftraggeber in angemessener Form mitzuteilen.
5. Der Auftragnehmer stellt sicher, dass die Umsetzung der technischen und organisatorischen Maßnahmen in seinem Verantwortungsbereich erfolgt und dass die mit der Verarbeitung betrauten Personen entsprechend verpflichtet und geschult sind.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer stellt sicher, dass die Verarbeitung personenbezogener Daten unter Beachtung der jeweils geltenden datenschutzrechtlichen Anforderungen erfolgt und seine interne Organisation entsprechend ausgestaltet ist.
2. Der Auftragnehmer stellt sicher, dass nur solche Personen Zugang zu personenbezogenen Daten erhalten, die zur Durchführung der Auftragsverarbeitung benötigt werden und zur Vertraulichkeit verpflichtet sind.
3. Der Auftragnehmer gewährleistet eine dem Stand der Technik entsprechende Sensibilisierung der mit der Verarbeitung betrauten Personen hinsichtlich Datenschutz und Datensicherheit.
4. Soweit gesetzlich erforderlich, bestellt der Auftragnehmer einen Datenschutzbeauftragten und teilt dessen Kontaktdaten dem Auftraggeber mit.

5. Eine Verarbeitung in Drittländern erfolgt nur unter Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage von Angemessenheitsbeschlüssen oder geeigneten Garantien (EU-Standardvertragsklauseln SCC).
6. Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihre bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Der Auftragnehmer benennt einen Ansprechpartner, der den Auftraggeber bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Auftraggeber dessen Kontaktdaten unverzüglich mit. Soweit der Auftraggeber besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragnehmer den Auftraggeber hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
7. Der Auftragnehmer unterstützt den Auftraggeber in angemessenem Umfang bei der Erstellung und Aktualisierung von Verarbeitungsverzeichnissen, der Durchführung einer Datenschutz-Folgeabschützung sowie bei der Zusammenarbeit mit Aufsichtsbehörden gem. Art. 35 und 36 DSGVO.
8. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die für den Nachweis der Einhaltung der datenschutzrechtlichen Verpflichtungen erforderlichen Informationen zur Verfügung. Eine Verpflichtung zur Offenlegung interner Verzeichnisse von Verarbeitungstätigkeiten besteht nicht, soweit diese über die zur Vertragserfüllung erforderlichen Informationen hinausgehen.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

1. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Beauftragung von Unterauftragnehmern im Rahmen der Verarbeitung personenbezogener Daten.
2. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragnehmer ergeben sich aus Anhang 2. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen dieser Liste, insbesondere über Hinzuziehung, Austausch oder Entfernung in geeigneter Weise.
3. Der Auftraggeber ist berechtigt, einer solchen Änderung aus nachvollziehbaren datenschutzrechtlichen Gründen innerhalb einer Frist von 14 Tagen nach Zugang der Information zu widersprechen.
4. Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt.
5. Im Falle eines berechtigten Widerspruchs werden die Parteien eine einvernehmliche Lösung anstreben. Sofern eine solche nicht innerhalb angemessener Frist erzielt werden kann, ist jede Partei berechtigt, den Vertrag aus wichtigem Grund zu kündigen. Im Falle einer solchen Kündigung werden bereits im Voraus gezahlte Entgelte zeitanteilig für die nicht in Anspruch genommenen Leistungen erstattet.
6. Der Auftragnehmer stellt sicher, dass mit allen Unterauftragnehmern vertragliche Vereinbarungen geschlossen werden.

Diese verpflichten den Unterauftragnehmer mindestens zu den gleichen datenschutzrechtlichen Pflichten wie in diesem Vertrag vorgesehen. Dies umfasst insbesondere die Verpflichtung zur Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung sowie zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen.

7. Ein Zugriff auf personenbezogene Daten durch den Unterauftragnehmer darf erst erfolgen, nachdem der Auftragnehmer durch geeignete vertragliche und organisatorische Maßnahmen sichergestellt hat, dass die in diesem Vertrag festgelegten datenschutzrechtlichen Pflichten eingehalten werden. Die in Anhang 2 zum Zeitpunkt des Vertragsschlusses benannten Unterauftragnhmer gelten als genehmigt, sofern die Voraussetzungen dieses § 5 erfüllt sind. Dies umfasst insbesondere die Sicherstellung angemessener Garantien im Sinne der DSGVO für eine rechtmäßig und sichere Verarbeitung personenbezogener Daten.
8. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten der Unterauftragnehmer verantwortlich.

§ 6 Kontrollrechte des Auftraggebers

1. Der Auftragnehmer stellt dem Auftrageber auf Anfrage alle erforderlichen Informatonen zur Verfügung, die zum Nachweis der Einhaltung der in diesem Vertrag sowie in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind.

2. Der Nachweis erfolgt vorrangig durch geeignete Unterlagen, insbesondere aktuelle Zertifizierungen (z.B. IT-Grundschutz, ISO 27001), Auditberichte (z.B. SOC 2), Dokumentation der technischen und organisatorischen Maßnahmen.

3. Der Auftraggeber kann darüber hinaus Kontrollen durchführen oder durch Dritte durchführen lassen, sofern der Dritte nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Kontrollen sind zulässig, sofern ein konkreter Anlass hierfür besteht oder die bereitgestellten Nachweise erwiesenermaßen nicht ausreichen.

4. Kontrollen vor Ort in den Geschäftsräumen des Auftragnehmers sind nur zulässig, soweit sie erforderlich sind, den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen und soweit sie mit angemessener Frist von mindestens 14 Tagen angekündigt werden.

5. Der Auftragnehmer ist berechtigt, im Rahmen von Kontrollen angemessene Maßnahmen zum Schutz von Geschäftsgeheimnissen, sicherheitsrelevanten Informationen sowie personenbezogenen Daten Dritter zu treffen. Insbesondere kann der Auftragnehmer Einsichtnahmen auf relevante Informationen beschränken, Unterlagen ganz oder teilweise schwärzen oder auf andere Weise unkenntlich machen und den Zugang zu bestimmten Systemen oder Räumlichkeiten verweigern, sofern dies zum Schutz der vorgenannten Interessen erforderlich ist. Die Kontrollrechte des Auftraggebers dürfen hierdurch nicht unangemessen eingeschränkt werden.

6. Kontrollen sind grundsätzlich zu den üblichen Geschäftszeiten durchzuführen und auf die Geschäftsräume, Systeme und relevanten Prozesse des Auftragnehmers beschränkt.

7. Kontrollen in privaten Wohnräumen sowie sonstigen nicht dem Auftragnehmer zuzurechnenden Räumlichkeiten von Mitarbeitern sind ausgeschlossen. Soweit Mitarbeiter des Auftragnehmers außerhalb der Geschäftsräume des Auftragnehmers tätig sind, stellt der Auftragnehmer durch

geeignete technische und organisatorische Maßnahmen sicher, dass die Anforderungen dieses Vertrags auch in diesen Arbeitsumgebungen eingehalten werden.

8. Der Auftraggeber trägt die Kosten der Kontrolle. Bei außergewöhnlichem Aufwand ist der Auftragnehmer berechtigt, eine angemessene Vergütung zu verlangen.

§ 7 Mitzuteilende Verstöße des Auftragnehmers

1. Der Auftragnehmer informiert den Auftraggeber ohne schuldhaftes Zögern, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO bekannt geworden ist, die Daten des Auftraggebers betrifft.

2. Die Mitteilung nach Absatz 1 enthält, soweit zum Zeitpunkt der Meldung verfügbar, eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Anzahl der betroffenen Personen sowie die Kategorien und die ungefähre Anzahl betroffener Datensätze, die hieraus resultierenden wahrscheinlichen Folgen sowie vorgeschlagene, erfgriffene und geplante Maßnahmen zur Behebung der Verletzung und zur Minderung möglicher nachteiliger Auswirkungen.

3. Sofern und soweit die Informationen nach Absatz 2 nicht gleichzeitig bereitgestellt werden können, stellt der Auftragnehmer diese Informationen schrittweise und ohne unangemessene Verzögerung zur Verfügung, sobald diese verfügbar sind.

4. Der Auftragnehmer ergreift unverzüglich geeignete Maßnahmen zur Sicherung der Daten und Minderung möglicher nachteiliger Folgen und stimmt weitere Maßnahmen mit dem Auftraggeber ab.

5. Der Auftragnehmer unterstützt den Auftraggeber in angemessenem Umfang bei der Erfüllung seiner Meldepflichten gem. Art. 33, 34 DSGVO, insbesondere bei der Erstellung von Meldungen an die Aufsichtsbehörde sowie bei der Information betroffener Personen.

6. Meldungen an Aufsichtsbehörden oder betroffene Personen durch den Auftragnehmer erfolgen ausschließlich nach vorheriger Weisung des Auftraggebers, es sei denn, der Auftragnehmer ist gesetzlich hierzu verpflichtet.

7. Der Auftragnehmer stellt dem Auftraggeber auf Anfrage im Zusammenhang mit einer Datenschutzverletzung weitere Informationen in angemessenem Umfang zur Verfügung, soweit dies zur Erfüllung gesetzlicher Pflichten erforderlich ist.

8. Eine Meldung stellt kein Schuldanerkenntnis dar.

9. Der Auftragnehmer informiert den Auftraggeber ebenfalls ohne schuldhaftes Zögern über erhebliche Störungen des Betriebsablaufs, Sicherheitsvorfälle oder sonstige Umstände, die die Sicherheit der Daten des Auftraggebers beeinträchtigen können.

10. Sollten personenbezogene Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, insbesondere Pfändung, Beschlagnahme, Insolvenzverfahren oder sonstige Ereignisse,

gefährdet werden, hat der Auftragnehmer den Auftraggeber ohne schuldhaftes Zögern hierüber zu informieren, sofern ihm dies rechtlich möglich ist. Der Auftragnehmer wird alle zuständigen Stellen darauf hinweisen, dass die Daten im Verantwortungsbereich des Auftraggebers stehen.

§ 8 Beendigung des Auftrags

1. Nach Beengigung der Verarbeitung wird der Auftragnehmer personenbezogene Daten nach Wahl des Auftraggebers löschen oder zurückgeben, sofern keine gesetzliche Aufbewahrungspflicht besteht.
2. Backups werden im Rahmen der üblichen Backup-Zyklen überschrieben und spätestens innerhalb von 90 Tagen gelöscht.
3. Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Haftung

1. Die Parteien haften im Rahmen der gesetzlichen Vorschriften.

2. Soweit gesetzlich zulässig, ist die Haftung des Auftragnehmers für leichte Fahrlässigkeit auf den vertragstypischen, vorhersehbaren Schaden begrenzt.

3. Der Auftraggeber stellt den Auftragnehmer im Innenverhältnis von Ansprüchen betroffener Personen frei, soweit die schadensursächliche Pflichtverletzung aus dem Verantwortungsbereich des Auftraggebers stammt. Die gesetzlichen Haftungsregelungen, insbesondere Art. 82 DSGVO, bleiben unberührt.

§ 10 Schlussbestimmungen

1. Die Vertragsbegründung, Vertragsänderungen und Nebenabreden bedürfen mindestens der elektronischen Form. Dies gilt auch für die Aufhebung dieses Formerfordernisses. Die elektronische Form umfasst insbesondere die Nutzung qualifizierter elektronischer Signaturen oder gleichwertiger elektronischer Signaturverfahren über gängige E-Signatur-Dienste.
2. Sollten einzelne Teile dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame oder undurchführbare Bestimmung durch eine wirksame erstetzen, die dem wirtschaftlichen Zweck der ursprünglichen Regelung möglichst nahekommt.

Auftraggeber:
Ort:
Datum:

Unterschrift:

Auftragnehmer:
Ort: Würzburg
Datum:

Unterschrift:

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung

Der Auftraggeber nutzt die Softwarelösungen des Auftragnehmers zur Unterstützung der Erfassung, Verarbeitung, Anreicherung, Validierung und Synchronisation von geschäftlichen Kontakt- und Stammdaten.

Dies umfasst:

- Die Erfassung von Kontaktdaten aus Visitenkarten, E-Mails, digitalen Quellen oder anderen vom Auftraggeber bereitgestellten oder öffentlich zugänglichen Informationsquellen
- Die Anreicherung von Validierung bestehender Datenbestände
- Die Übertragung und Synchronisation von Daten in CRM- oder sonstige vom Auftraggeber genutzte Systeme
- Die Erstellung und Verarbeitung von Besuchs- und Gesprächsberichten im Rahmen von Geschäftsbeziehungen, insbesondere bei Messen, Veranstaltungen oder Kundenbesuchen
- Die Bereitstellung digitaler Visitenkarten zur Übermittlung eigener geschäftlicher Kontaktdaten durch Nutzer des Auftraggebers

Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt zur

- strukturierten elektronischen Erfassung, Verarbeitung und Pflege geschäftlicher Kontaktdaten,
- Verbesserung der Datenqualität durch Validierung, Aktualisierung und Anreicherung
- Integration und Synchronisation von Daten mit Systemen des Auftraggebers (insbesondere CRM-Systeme)
- Unterstützung vertrieblicher und geschäftlicher Kommunikationsprozesse
- Dokumentation geschäftlicher Kontakte und Interaktionen

Die Verarbeitung erfolgt mittels webbasierter Anwendungen, mobiler Endgeräte sowie Schnittstellen (API) zwischen Systemen des Auftraggebers und des Auftragnehmers

Art der personenbezogenen Daten	Verarbeitet werden folgende Kategorien personenbezogener Daten: — Identifikations- und Kontaktdaten (Vorname, Nachname, Titel) — Berufliche Kontaktdaten (E-Mail-Adresse, Telefonnummer, Faxnummer) — Geschäftliche Adressen (Unternehmen, Firma, Abteilung, Position, Straße, Hausnummer, PLZ, Ort, Land) — sowie weitere berufliche oder organisationsbezogene Angaben, die im Rahmen der genannten Datenquellen typischerweise auf Visitenkarten, in öffentlichen beruflichen Profilen oder durch den Auftraggeber bereitgestellt werden und in unmittelbarem Zusammenhang mit der geschäftlichen Kontaktaufnahme stehen Eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Gegenstand der Verarbeitung.
Kategorien betroffener Personen	Von der Verarbeitung betriffen sind — Kunden und potenzielle Kunden des Auftraggebers — Geschäftspartner und Lieferanten — Interessenten und Leads — Teilnehmer auf Messen, Veranstaltungen und Geschäftsterminen — Mitarbeiter und Ansprechpartner von Kunden, Interessenden und Gesprächspartnern — sowie sonstige natürliche Personen, deren geschäftliche Kontaktdaten im Rahmen konkreter geschäftlicher Kommunikations- oder Beziehungsanlässe durch den Auftraggeber in das System eingebracht und dort verarbeitet werden, soweit dies zur geschäftlichen Kommunikation, Anbahnung oder Durchführung von Vertrags- oder Geschäftsbeziehungen erforderlich ist
Name und Kontaktdaten des Datenschutzbeauftragten des Auftraggebers (sofern benannt):	Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:
Auftraggeber: E-Mail: Telefon:	**SiDIT GmbH** E-Mail: legal@snapaddy.com Telefon: +49 931 780877 0

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungs-standort**	**Art der Dienstleistung**
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	AWS Region Frankfurt, Deutschland (eu-central-1)	Bereitstellung von Infrastrukturleistungen (Cloud-Hosting, Datenverarbeitung und Speicherleistungen im Rahmen eines Rechenzentrumsbetriebs)
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland	europe-west3-Region, Frankfurt	Bereitstellung von Cloud-Diensten zur Datenverarbeitung und Analyse von Daten, einschließlich Texterkennung (OCR)
Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	swedencentral (Gävle, Sandviken und Staffanstorp, Schweden), germany-westcentral (Frankfurt am Main, Deutschland), westeurope (Amsterdam, Niederlande)	Bereitstellung von Cloud-Infrastruktur- und Plattformdiensten, einschließlich Datenverarbeitung, einschließlich KI-gestützter Sprach- und Textverarbeitung sowie Speicher- und Hostingleistungen

Anhang 3: Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Im Zuge der Auftragsverarbeitung ergreift der Auftragnehmer folgende technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus.

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

a. Zutrittskontrolle

Maßnahmen zur Verhinderung des Zutritts Unbefugter zu Datenverarbeitungsanlagen:

- Elektronische Zutrittskontrolle im gesamten Gebäudekomplex
- Zutritt mittels zentraler Schließanlage für berechtigte Personen
- Verwaltung individueller Zutrittsprofile (zeitlich und räumlich eingeschränkt)
- Zutrittskontrolle zu Hosting-Systemen erfolgt durch den Subdienstleister (AWS) gemäß dessen zertifizierten Sicherheitsmaßnahmen (u. a. ISO 27001, SOC 2)

b. Zugangskontrolle

Maßnahmen zur Verhinderung der Nutzung von IT-Systemen durch Unbefugte:

- Einsatz von Firewall-Systemen, Anti-Malware-Lösungen und Proxy-Systemen
- Einheitliche Passwortrichtlinie:
  - mindestens 12 Zeichen
  - Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen
  - keine Wiederverwendung von Passwörtern
  - verpflichtende Nutzung eines Passwortmanagers
- Multi-Faktor-Authentifizierung (MFA):
  - verpflichtend für privilegierte Zugänge und kritische Systeme
  - Umsetzung ausschließlich über sichere Verfahren (z. B. TOTP-basierte Authenticator-Apps)
  - SMS-basierte Verfahren sind nicht zugelassen
- Mobile Geräte sind durch PIN (mind. 6-stellig) oder biometrische Verfahren geschützt
- Zugriff ausschließlich über verschlüsselte Verbindungen (TLS 1.2 / TLS 1.3 gemäß Stand der Technik, z. B. BSI TR-02102-2)

c. Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Berechtigte nur auf erforderliche Daten zugreifen:

- Rollenbasierte Zugriffskontrolle (RBAC) nach dem Least-Privilege-Prinzip
- „Deny by Default"-Ansatz (keine Berechtigung ohne explizite Freigabe)
- Rechtevergabe und -prüfung erfolgen regelmäßig (mind. jährlich, bei kritischen Systemen häufiger)
- Zugriff nur über personalisierte Benutzerkonten mit MFA
- Verschlüsselung von Daten und Datenträgern (AES-256)
- Kontinuierliches Monitoring der Systeme zur Erkennung unberechtigter Zugriffe
- Sicherheitslücken werden zeitnah identifiziert und behoben

d. Pseudonymisierung

Maßnahmen zur Trennung von Identifikationsmerkmalen:

- Einsatz von Pseudonymisierung, sofern technisch und organisatorisch sinnvoll (z. B. Tokenisierung)
- Trennung von Identifikationsdaten und Fachdaten
- Separate und geschützte Aufbewahrung der Zuordnungsinformationen
- Klare Abgrenzung zur Verschlüsselung:
  - Verschlüsselung (z. B. AES-256) dient dem Schutz der Vertraulichkeit
  - Pseudonymisierung reduziert die direkte Personenbeziehbarkeit

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

a. Weitergabekontrolle

Maßnahmen zur Sicherstellung sicherer Datenübertragung:

- Datenübertragung ausschließlich verschlüsselt (TLS 1.2 / TLS 1.3)
- Verwendung sicherer Cipher Suites gemäß Stand der Technik
- Verschlüsselung von Datenträgern
- Berechtigungskonzept für Datenübermittlung, -änderung und -löschung
- Vertragliche Verpflichtung aller Mitarbeitenden auf Vertraulichkeit
- Zugriffsbeschränkungen beim Hosting-Dienstleister durch technische und organisatorische Maßnahmen (z. B. Verschlüsselung, Netzwerksegmentierung, Zertifizierungen)

b. Eingabekontrolle

Maßnahmen zur Nachvollziehbarkeit von Datenverarbeitung:

- Protokollierung aller Eingaben, Änderungen und Löschungen personenbezogener Daten
- Zuordnung zu individuellen Benutzerkonten
- Zugriff auf Protokolle nur für berechtigtes Personal

c. Logging und Monitoring

Maßnahmen zur Überwachung und Erkennung sicherheitsrelevanter Ereignisse:

- Zentrale Erfassung von Log-Daten (z. B. System-, Audit- und Cloud-Logs)
- Definition von Verantwortlichkeiten, Speicherorten und Aufbewahrungsfristen
- Regelmäßige Auswertung der Logs
- Automatisierte Erkennung von Anomalien
- Übergabe sicherheitsrelevanter Ereignisse an Incident-Management-Prozesse

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

a. Verfügbarkeitskontrolle

Maßnahmen zum Schutz vor Datenverlust:

- Dokumentiertes Backup- und Recovery-Konzept
- Regelmäßige Datensicherungen (z. B. tägliche Backups)
- Definierte Aufbewahrungsfristen (z. B. 30 Tage)
- Regelmäßige Wiederherstellungstests (mind. jährlich)
- Zielparameter:
  - RPO (Recovery Point Objective): max. 24 Stunden
  - RTO (Recovery Time Objective): max. 1 Geschäftstag
- Verschlüsselte Speicherung von Backups (AES-256)

— Nutzung hochverfügbarer Rechenzentren (AWS) mit physischer Absicherung (z. B. Brand- und Umweltschutz)

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

a. Auftragskontrolle

— Verarbeitung personenbezogener Daten ausschließlich gemäß Art. 28 DSGVO und vertraglicher Weisung
— Kontroll- und Auditrechte des Auftraggebers werden unterstützt
— Nachweisführung über getroffene Maßnahmen
— Absicherung von Subdienstleistern durch vertragliche Regelungen und Zertifizierungen

b. Trennungsgebot

— Logische Trennung von Daten unterschiedlicher Mandanten
— Trennung von Test- und Produktivumgebungen
— Keine Nutzung von Echtdaten in Testsystemen

c. Datensicherheitsmanagement

— Betrieb eines Informationssicherheitsmanagementsystems (ISMS), z. B. nach ISO 27001
— Regelmäßige Überprüfung und Weiterentwicklung der Sicherheitsmaßnahmen
— Versionierung und Aktualisierung der TOM-Dokumentation

d. Datenschutzfreundliche Voreinstellungen (Privacy by Default)

— Umsetzung des „Deny by Default"-Prinzips
— Minimalprinzip bei Datenerhebung und -verarbeitung
— Zugriff nur im erforderlichen Umfang (Least Privilege)
— Regelmäßige Überprüfung von Berechtigungen

e. Risikomanagement

— Kontinuierliche Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen
— Anpassung der Schutzmaßnahmen entsprechend Risikolage, Stand der Technik und Verarbeitungskontext

f. Patch- und Schwachstellenmanagement

— Zeitnahe Installation von Sicherheitsupdates
— Strukturierter Patch-Management-Prozess
— Kontinuierliche Überwachung von Schwachstellen (z. B. über Sicherheitsquellen und Tools)
— Bewertung und Behandlung identifizierter Risiken
— Durchführung regelmäßiger Sicherheitstests (z. B. Penetrationstests)

5. Verschlüsselung und Schlüsselmanagement

— Verschlüsselung von Daten „at rest" (z. B. AES-256 bei Datenbanken und Storage-Systemen)

— Verschlüsselung „in transit“ über TLS 1.2 / 1.3
— Zentrales Schlüsselmanagement (z. B. KMS)
— Zugriff auf kryptographische Schlüssel streng reglementiert

Stand: Juni 2026

Anhang 4: Weisungsberechtigte Personen

Der Auftraggeber benennt die zur Erteilung von Weisungen berechtigten Personen. Änderungen sind dem Auftragnehmer unverzüglich mindestens in Textform mitzuteilen. Weisungen gelten nur dann als verbindlich erteilt, wenn sie von den benannten Personen erteilt wurden.

Weisungsberechtigte Personen des Auftraggebers sind:

Name:
Position:
E-Mail:

Name:
Position:
E-Mail:

Anhang 5: Drittlandtransfer

Sofern der Auftragnehmer personenbezogene Daten in ein Drittland übermittelt oder ein Unterauftragnehmer in einem Drittland eingesetzt wird, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO.

Hierzu werden, sofern kein Angemessenheitsbeschluss vorliegt, die Standardvertragsklauseln der Europäischen Kommission (Durchführungsbeschluss (EU) 2021/914) angewendet.

Die Parteien vereinbaren, dass in diesem Fall die jeweils anwendbaren Module der Standardvertragsklauseln automatisch Bestandteil dieses Vertrags werden.