LIMTEC
Server-Management & Web-Entwicklung
Halderstr. 16
86150 Augsburg
www.limtec.de
Mail info@limtec.de
Fax +49 821 - 32871103
Tel +49 821 - 32872895

Auftragsverarbeitungs (AV)-Vertrag nach Art. 28 DS-GVO

Inhalt Version 1.2 (20.07.2020)

Auftrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zwischen

_____

- Verantwortlicher - nachstehend Auftraggeber genannt

und

LimTec GmbH, Halderstr. 16, 86150 Augsburg

_____

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

1. Gegenstand und Dauer bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben.
   Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Artikel 4 Nummer 2 bzw Artikel 28 der DSG-VO.
2. Dieser Vertrag gilt, sofern keine anderweitigen Regelungen vereinbart wurden, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet. Dieser Vertrag ersetzt evtl bereits vorhandene vorhergehende Verträge zur Auftragsdatenverarbeitung zwischen den Vertragsparteien.

2. Konkretisierung des Auftragsinhalts

1. Art und Zweck der Verarbeitung oder Nutzung personenbezogener Daten, sowie der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in 1.1) beschriebenen Vertragsverhältnisse ergibt.
2. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen

1. 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 zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten

Maßnahmen Grundlage des Auftrags.

2. Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen (Einzelheiten in Anlage 2).
3. 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. Berichtigung, Einschränkung und Löschung von Daten

1. 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.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

1. Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
    a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
    Als Datenschutzbeauftragte ist beim Auftragnehmer
    Herr Heiner Dassow, 0821 - 32871103, datenschutz@limtec.de bestellt.
    Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
    b. Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.
    c. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f. 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.
g. 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.
h. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

1. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. 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.
2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.
3. Der Auftraggeber stimmt der Beauftragung der in Anlage 3 dargestellten Unterauftragnehmer zu. Die Rechte der durch die Datenverarbeitung betroffenen Personen sind vom Auftragnehmer auch gegenüber dem Unterauftragnehmer geltend zu machen.
4. 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.

7. Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der

Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.
3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
    a. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
    b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
    c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
    d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.
    a. die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
    b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
    c. 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
    d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
    e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

1. 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.
2. 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.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

1. Diese Vereinbarung gilt nur in Verbindung mit einem Hauptvertragsverhältnis gemäß Ziffer 1. Die Kündigung oder Beendigung des Hauptvertragsverhältnisses beendet gleichzeitig diese Vereinbarung.
   Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.
2. Es gilt das Recht der Bundesrepublik Deutschland.
3. Die Parteien vereinbaren als Gerichtsstand den Sitz des für Augsburg zuständigen Gerichts.

_____	_____
Ort/Datum	Ort/Datum
_____	_____
Unterschrift Auftraggeber (Kunde)	Unterschrift Auftragnehmer

Anlage 1: Art der Daten und betroffener Personenkreis

Auflistung Art und Zweck der Verarbeitung oder Nutzung personenbezogener Daten:

1. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- O Personenstammdaten
- O besonders schützenswerte Personendaten gemäß Art. 9 DS-GVO (bitte angeben)

- O Kommunikationsdaten (z.B. Telefon, Fax, Email)
- O Vertragsstammdaten
- O Protokolldaten
- O weitere (bitte angeben)

2. Kategorie betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- O Kunden und Interessenten des Auftraggebers
- O Mitarbeiter und Lieferanten des Auftraggebers
- O weitere (bitte angeben)

Anlage 2 - Technisch organisatorische Maßnahmen

Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**

  alle Rechenzentren:
  - Videoüberwachung im Innen und Aussenbereich
  - PIN-geschützte Zugangsbereiche
  - elektronisches Zutrittskontrollsystem
  - Alarmanlage

  LimTec Colocation Unterschleissheim:
  - Zutritt nur in Begleitung von autorisierten Fachpersonal

  e-shelter Rechenzentrum:
  - Zutrittskontrolle nach ISO-27001 und ISO-9001 zertifiziert

- **Zugangskontrolle**

  Managed-Server und Webhosting:
  - passwortgeschützter Benutzer-Zugang zu Server und Kundenmenü
  - Vergabe hinreichend langer Zufallspasswörter
  - Administrativer Zugriff nur für berechtigte Mitarbeiter vom Auftragnehmer

  Root-Server und Server im Eigentum des Auftraggebers:
  - Für die Einhaltung der Zugangskontrolle ist der Auftraggeber verantwortlich

  interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
  - Vergabe hinreichend langer Zufallspasswörter
  - Zugriff auf kritische Systeme über VPN
  - Einsatz von Datenträgerverschlüsselung wo sinnvoll und erforderlich (z.B. mobile Datenträger)

  weitere Maßnahmen werden nach Bedarf eingesetzt, u.a.
  - Datenträgerverschlüsselung
  - BruteForce Detection mit automatischer Sperrung
  - Protokollierung der Zugriffe

- **Zugriffskontrolle**

  Managed-Server und Webhosting:
  - regelmäßige Sicherheitsupdates des Betriebssystems und der vom Auftraggeber verwalteten Software sofern diese über ein öffentliches Netz erreichbar sind
  - Erreichbarkeit nur über ein internes Netz, falls regelmäßige Sicherheitsupdates aufgrund von Kompatibilitäts- oder Verfügbarkeitsanforderungen nicht erfüllt werden können

- für vom Auftraggeber übertragene und/oder verwaltete Software/Daten ist der Auftraggeber auch für deren Sicherheit und Updates zuständig

Root-Server und Server im Eigentum des Auftraggebers:
- Für die Einhaltung der Zugriffskontrolle ist der Auftraggeber verantwortlich

interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
- Betrieb in einem internen Netz (Zugriff via VPN)
- Einsatz von zentralen Monitoring

weitere Maßnahmen werden nach Bedarf eingesetzt, u.a.
- zentrales Monitoring
- zentrales Ausbringen von Updates via Puppet
- Vermeidung unberechtigter Zugriffe (Web Application Firewall, DDOS-Blocker, Firewall, Proxy)
- Detektion kompromittierter Kundenanwendungen (Virenscan, Prozessüberwachung)

- **Trennungskontrolle**

Managed-Server und Webhosting:
- physisch oder logische getrennte Produktiv- und Testsysteme
- physisch oder logische Trennung von Daten
- Datensicherung auf physisch oder logisch getrennte Systeme

Root-Server und Server im Eigentum des Auftraggebers:
- Für die Trennungskontrolle ist der Auftraggeber verantwortlich

interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
- physisch oder logische Trennung von Daten
- Datensicherung auf physisch oder logisch getrennte Systeme
- Projekt-/Aufgabenbezogener Mitarbeiter- oder Kundenzugriff

weitere Maßnahmen werden nach Bedarf eingesetzt, u.a.
- Trennung der Netze in verschiedene Sicherheitsbereiche (teilweise nur über VPN zugänglich)
- Sandboxing oder Separierung mittels Virtualisierungstechnik

- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Managed-Server und Webhosting:
- Zugriffslogs und Statistiken werden anonymisiert gespeichert und nach 180 Tagen gelöscht
- Der Auftraggeber ist für die Pseudonymisierung von Anwendungsdaten zuständig

Root-Server und Server im Eigentum des Auftraggebers:
- Der Auftraggeber ist für die Pseudonymisierung zuständig

interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
- Anonymisierung der Logs wo erforderlich

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**

  Managed-Server und Webhosting:
  - verschlüsselte Datenübertragung (unterstützte Protokolle sind der Leistungsbeschreibung zu entnehmen, i.d.R. SSH, SCP, SFTP, HTTPS)
  - verschlüsselte Übertragung von Backups
  - Bereitstellung kostenloser Letsencrypt-Zertifikate

  Root-Server und Server im Eigentum des Auftraggebers:
  - Der Auftraggeber ist für die Weitergabekontrolle zuständig

  interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
  - verschlüsselte Datenübertragung
  - verschlüsselte Übertragung von Backups
  - Mitarbeiter sind der Einhaltung des Datenschutzes verpflichtet
  - Nutzung von VPN (nach Bedarf)

- **Eingabekontrolle**

  Managed-Server und Webhosting:
  - Änderungen der Daten werden protokolliert
  - Der Autraggeber ist für die Eingabekontrolle innerhalb seiner Anwendungen zuständig

  Root-Server und Server im Eigentum des Auftraggebers:
  - Der Auftraggeber ist für die Eingabekontrolle zuständig

  interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
  - Nutzer müssen sich vor Eingabe authentifizieren
  - Änderungen der Daten werden protokolliert

  weitere Maßnahmen werden nach Bedarf eingesetzt, u.a.
  - Protokollierung von Änderungen über ein Versions-Management System
  - Protokollierung von Änderungen über ein Change-Management System

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

  Managed-Server und Webhosting:
  - Backup-Konzept mit täglicher Sicherung (abhängig vom gewählten Tarif)
  - Einsatz von Schutzprogrammen (Web Application Firewall, DDOS-Blocker, Firewall, Proxy, Spam-Filter)

  Root-Server und Server im Eigentum des Auftraggebers:
  - Die Datensicherung obliegt dem Auftraggeber

interne Systeme des Auftragnehmers (Infrastruktur, zentrale Dienste, Verwaltung):
  - Backup-Konzept mit täglicher Sicherung
  - Einsatz von Schutzprogrammen (Web Application Firewall, DDOS-Blocker, Firewall, Proxy, Spam-Filter)

weitere Maßnahmen werden nach Bedarf eingesetzt, u.a.
  - zentrales Monitoring
  - Einsatz unterbrechungsfreier Stromversorgung und Netzersatzanlage
  - Einsatz redundanter Klimatechnik
  - Einsatz redundanter Netzanbindung
  - Einsatz von Festplattenspiegelung
  - Einsatz verteilter Speichertechnologien (DRBD, CEPH)

- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DS-GVO);

  - Möglichkeit zur schnellen Verlagerung von Servern und Diensten an einem anderen Rechenzentrums-Standort (internes Netz über zwei Standorte)
  - Möglichkeit zur Live-Migration virtualisierter Server auf andere Hostsysteme
  - Einsatz von Fallback-Hardware für die Wiederinbetriebnahme bei Hardwareproblemen
  - Maßnahmen zum schnellen Bereitstellen neuer Server (u.a. automatisierte Installation via Puppet und Vereinheitlichung von Systemimages)
  - schneller Zugriff auf Backupdaten durch Snapshots

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**

  - Einführung eines Datenschutz-Management-Systems

- **Incident-Response-Management**

  - Ticket-System für Fehlerreporting
  - zentrales Monitoringsystem
  - Notfallhotline

- **Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO);

  Datenschutzfreundliche Voreinstellungen sind wesentlicher Bestandteil aller internen Softwareentwicklungen.

  abhängig vom gewählten Tarif:
  - Anonymisierung von IP-Adressen voreingestellt
  - Standardmäßig aktivierte Sicherheitsfunktionen (Web Application Firewall, DDOS-Blocker, Firewall, Viren-Scanner und Spam-Filter)
  - kostenlose Letsencrypt SSL-Zertifikate

- **Auftragskontrolle**

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 3: Liste der Unterauftragnehmer

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte und der erbrachten Leistungen:

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
mes.mo GmbH	Stuttgarter Str. 4 D-73262 Reichenbach	SMS-Versand (für Freischaltcode)
Hostway Deutschland GmbH	Am Mittelfelde 29 D-30519 Hannover	Registrierung von Domainnamen
SaSG GmbH & Co. KG	Cecinastraße 70 D-82205 Gilching	Connectivity, Gebäudetechnik Rechenzentrum Unterschleißheim
e-shelter services GmbH	Eschborner Landstraße 100 D-60489 Frankfurt am Main	Connectivity, Gebäudetechnik Rechenzentrum e-Shelter
Hetzner Online GmbH	Industriestr 25 D-91710 Gunzenhausen	Server-Dienstleistungen