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

meetzi - Auftragsverarbeitungs (AV)-Vertrag nach Art. 28 DS-GVO
Version 3 (14.12.2020)

Inhalt

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 der Verarbeitung

1. **Gegenstand**

   Gegenstand des Auftrags zur Datenverarbeitung sind die folgenden Dienstleistungen:

   a) Bereitstellung und Betrieb eines webbasierten virtuellen Konferenzsystems unter der Domain https://meetzi.de, https://klassenzimmer.meetzi.de oder unter einer vom Auftraggeber bereitgestellten Domain,
   b) Bereitstellung und Betrieb der dazugehörigen Serversysteme,
   c) Erbringung von Support- und Fernwartungsleistungen.

   Die vertraglich vereinbarte Dienstleistung wird ausschließlich in Deutschland erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein anderes Land bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2. **Dauer der Verarbeitung**

   Die Datenverarbeitung beginnt mit der Auftragsvergabe und wird auf unbestimmte Zeit beschlossen. Die Vertragslaufzeit beträgt 3 Monate und verlängert sich zum Laufzeitende jeweils um denselben Zeitraum. Die Kündigungsfrist beträgt 2 Wochen zum jeweiligen Laufzeitende.
   Sofern davon abweichende Vereinbarungen zu Vertragslaufzeit und Kündigungsfrist getroffen werden, werden diese schriftlich im Auftrag dokumentiert.

   Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen

Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der Daten sowie Kategorien betroffener Personen

1. **Art und Zweck der Verarbeitung**

   Zweck der Verarbeitung ist die Bereitstellung von virtuellen Konferenzräumen mit Audio/Video-Konferenz, Chat, Dateiaustausch sowie integrierten Planungs- und Dokumentationswerkzeugen.

   Der Auftragnehmer verarbeitet personenbezogene Daten im Einklang mit den Bestimmungen der Europäischen Datenschutz-Grundverordnung (DSGVO).

   Der Auftragnehmer verpflichtet sich dazu, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Dienstleistungen zu verwenden.

2. **Art der Daten**

   Folgende Daten sind Bestandteil der Datenverarbeitung:

   - Personenstammdaten
   Name oder Pseudonym der Teilnehmer,

   - Kommunikationsdaten der Nutzer der Plattform
   IP-Adressen, Audio/Video-Daten, Chatnachrichten der Teilnehmer,

   - Protokolldaten (Server-Logfiles) der Nutzer der Plattform
   Zugriffskontrolle und -überwachung,

   - Sonstige Daten (Dokumente, Bilder und Grafiken) der Nutzer der Plattform
   von den Teilnehmern hochgeladene oder im virtuellen Konferenzraum erstellte Daten.

3. **Kategorien betroffener Personen**

   Von der Verarbeitung betroffene Personen sind:

   - Nutzer der Plattform (Lehrer/Moderatoren),
   - durch den Lehrer/Moderator eingeladene Teilnehmer,
   - Personen, über die kommuniziert wird.

3. Pflichten des Auftragnehmers

1. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des Auftrages und auf Weisung des Auftraggebers verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Kopien oder Duplikate zu erstellen (z.B. Datensicherungen, Caching, Log-Dateien etc.). Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (vgl. Anlage 1). Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

6. Beim Auftragnehmer ist als Ansprechpartner und Beauftragter für den Datenschutz Herr Heiner Dassow, 0821 - 32871103, datenschutz@limtec.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

8. Im Rahmen der beauftragten Dienstleistung verarbeitete Daten wird der Auftragnehmer auf Weisung des Auftraggebers aushändigen, berichtigen oder löschen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

9. Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen nach Wahl des Verantwortlichen entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht. Die Löschung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Die Datenverarbeitung durch den Auftragnehmer findet ausschließlich in Ländern statt, die der Europäischen Union oder dem Europäischen Wirtschaftsraum (EU/EWR) angehören.

4. Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung und die Wahrung der Rechte von Betroffenen ist der Auftraggeber verantwortlich.

2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind vom Auftragnehmer unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Weisungen, die über die vertraglichen Vereinbarungen hinaus gehen, können kostenpflichtig sein.

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

5. Anfragen betroffener Personen

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.
   Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart.
   Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

2. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem unmittelbaren Wettbewerbsverhältnis stehen.

3. Kontrollen beim Auftragnehmer dürfen nicht zu übermäßigen Beeinträchtigungen des Geschäftsbetriebs führen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

7. Subunternehmer

1. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Insbesondere trägt er Sorge dafür, dass der Unterauftragnehmer hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt. Der Auftragnehmer wird angemessene Überprüfungen und Inspektionen, im Bedarfsfall auch vor Ort, bei Subunternehmern durchführen oder durch von ihm beauftragte Dritte durchführen lassen.

2. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

3. Der Auftraggeber stimmt der Beauftragung der in Anlage 2 dargestellten Unterauftragnehmer zu.

8. Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten von der Datenverarbeitung betroffene Daten (vgl. 2.2) beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

2. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

3. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

4. Es gilt das Recht der Bundesrepublik Deutschland.

5. Die Parteien vereinbaren als Gerichtsstand den Sitz des für Augsburg zuständigen Gerichts.

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

Anlage 1 - 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

  Hetzner Rechenzentrum:
  - Zutrittskontrolle nach ISO-27001 zertifiziert

- **Zugangskontrolle**

  Managed-Server, Webhosting, Meetzi:
  - 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, Webhosting, Meetzi:
  - 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, Webhosting, Meetzi:
  - 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, Webhosting, Meetzi:
  - Zugriffslogs und Statistiken werden anonymisiert gespeichert und nach 180 Tagen gelöscht
  - Der Auftraggeber ist für die Pseudonymisierung von Anwendungsdaten zuständig, sofern er eigene Anwendungen einsetzt.

  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, Webhosting, Meetzi:
  - 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, Webhosting, Meetzi:
  - 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, Webhosting, Meetzi:
  - 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 2: Liste der Unterauftragnehmer

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

1. **SaSG GmbH & Co. KG**
   Cecinastraße 70, D-82205 Gilching
   LimTec mietet eigene Serverräume und nutzt die Gebäudetechnik (Klima, Notstrom, Netzwerkkomponenten). Die am Verarbeitungsstandort untergebrachten Server sind Eigentum der LimTec GmbH, Betrieb und Serverwartung (Hardware und Software) erfolgt durch die LimTec GmbH.

   Verarbeitungsstandort:
   SaSG GmbH & Co. KG, Max-Planck-Straße 1, D-85716 Unterschleißheim

2. **NTT Global Data Centers EMEA GmbH (früher e-shelter services GmbH)**
   Voltastraße 15, D-65795 Hattersheim am Main
   LimTec mietet eigene Server-Racks und nutzt die Gebäudetechnik (Klima, Notstrom, Netzwerkkomponenten). Die am Verarbeitungsstandort untergebrachten Server sind Eigentum der LimTec GmbH, Betrieb und Serverwartung (Hardware und Software) erfolgt durch die LimTec GmbH.

   Verarbeitungsstandort:
   e-shelter, Landshuter Str. 7, D-85716 Unterschleißheim

3. **Hetzner Online GmbH**
   Industriestr 25, D-91710 Gunzenhausen
   LimTec mietet Dedicated Root-Server. Betrieb und Serverwartung (Software) erfolgt durch die LimTec GmbH. Die am Verarbeitungsstandort untergebrachten Server sind Eigentum der Hetzner Online GmbH, die Wartung der Hardware erfolgt durch die Hetzner Online GmbH.

   Verarbeitungsstandort:
   Hetzner Online GmbH, Am Datacenter-Park 1, D-08223 Falkenstein/Vogtland