Auftragsverarbeitung
gemäß Artikel 28 Datenschutz-Grundverordnung

VARIAS GmbH
Bahnhofplatz 2
4600 Wels
FN 574364 d
als „**Auftragsverarbeiter** gemäß DSGVO

verpflichtet sich gegenüber dem Kunden (Lizenznehmer) als „Verantwortlicher" gemäß DSGVO wie folgt, wobei der dokumentierte Vertragsabschluss durch die auf der Homepage vorgenommene Bestätigung dieser Vertragsbedingungen erfolgt:

1. Präambel

Die Datenschutz-Grundverordnung („DSGVO") beschreibt die Rollen im Datenschutz aus organisatorischer Sicht und verpflichtet alle Verantwortlichen zum Abschluss einer dokumentierten oder schriftlichen Vereinbarung mit jedem Auftragsverarbeiter, der im Auftrag des Verantwortlichen personenbezogene Daten von natürlichen Personen verarbeitet.

Gemäß Art 28 DSGVO sind in der Vereinbarung u.a. Gegenstand und Zweck, Dauer und Ort der Verarbeitung, Art und Kategorien der personenbezogenen Daten, Vertraulichkeit, Sicherheitsmaßnahmen, Löschung, Auskunftsrechte zu nennen und festzulegen.

Zur Entsprechung dieser Anforderung gilt, ergänzend zum VARIAS Lizenzmietvertrag als Hauptvertrag diese Verpflichtung als integrierter Bestandteil.

Im Weiteren bezeichnet die Begriffe

a. „**Hauptvertrag**", Lizenz Mietverträge für folgende Softwaremodule:

- VARIAS Vorsorgerechner (Berechnung von Vorsorgelücken)
- VARIAS Tarifrechner (Berechnung von Tarifvergleichen)
- BEPRO Beratungsprozess (digitaler Kundenberatungsprozess)
- Bedarfsanalyse (zur Integration in die Kundenwebseite
- Public Pensionsrechner (zur Integration in die Kundenwebseite)
- VARIASsign– elektronische Unterschriftslösung

b) „**DSGVO**" die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung)

c) **Verantwortlicher**: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

d) **Auftragsverarbeiter**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

e) **Verarbeitung**: bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form

der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

2. Gegenstand und Zweck der Verarbeitung

(1) Gegenstand der Verarbeitung sind ausschließlich jene Daten, welche für die Erfüllung des jeweiligen Hauptvertrages erforderlich oder zweckdienlich sind. Es werden außer diesen Daten keine weiteren Daten verarbeitet. Die Daten werden ausschließlich vom Verantwortlichen im vom Auftragsverarbeiter zur Verfügung gestellten System bereitgestellt und für dessen Zwecke verarbeitet.

(2) Im Einzelnen sind die teilweise oder gänzliche Durchführung einer oder mehrerer der folgenden Aufgaben Gegenstand des Hauptvertrages:

- VARIAS Vorsorgerechner:
  Berechnungsmöglichkeit für eine IDD konforme Darstellung der Vorsorgelücken im Bereich Alterspension (inkl. Berücksichtigung bestehender Vorsorgen), Berufsunfähigkeit (inkl. Reha- und Umschulungsgeld), Unfall Lücke sowie Todesfall Lücke (inkl. Witwen- und Waisenpension)

- VARIAS Tarifrechner:
  Vergleich von verschiedenen Versicherungen zu unterschiedlichen Versicherungsleistungen (Berufsunfähigkeitsversicherung, klassische Rentenversicherung, fondsgebundene Rentenversicherung und Risiko-Lebensversicherung), bei dem der Verantwortliche durch die Bekanntgabe von personenbezogenen Daten im Rahmen der Vertragsanbahnung von Versicherungsverträgen die Möglichkeit hat, unterschiedliche Versicherungen zu vergleichen. Nach Auswahl des gewünschten Vertragspartners für den Kunden kann durch einen Mausklick das fertig ausgefüllte PDF Angebot inkl. Antrag erstellt werden.

- BEPRO Beratungsprozess (digital)
  durchgehend geführter Prozess (Erstgespräch bis zum abschließenden Beratungsprotokoll), die Archivierung (Daten, Protokolle und Dokumenten), Zuweisung von Aufgaben, Anbindung an Standardanwendungen (z.B. Kundenverwaltung, den Tarifrechner, etc.)
- Bedarfsanalyse
  Erhebung von Wünschen und Bedürfnissen des Kunden über die Webseite mit einer optional integrierten Auswertung des empfohlenen Versicherungsschutzes.
- Public Pensionsrechner
  Einbindung eines Pensionsrechners in die Webseite des Kunden zur Ermittlung der voraussichtlichen Alters- und/oder Berufsunfähigkeitspension (mit Pensionskontologik)
- VARIASsign– elektronische Unterschriftslösung
  Hochgeladene Dokumente oder Dokumente, die von Fremdapplikationen mittels Schnittstelle an VARIASsign übergeben werden können mit Unterschriftsfelder der Signatoren versehen werden. Im Anschluss wird ein Link via SMS oder Email des Dokuments an den (die) Signator(en) mit der Aufforderung zur Unterschrift übermittelt. Eine Unterzeichnung direkt am Erstellungsgerät mittels Touchpads oder Signpads ist ebenfalls möglich. Nach erfolgter Unterschrift aller Signatoren kann ein Dokumentenlink an den Signator übermittelt werden.

3. Dauer der Verarbeitung

(1) Sofern eine Leistung im Einzelfall (Unterstützung, Support, Datenbankwartung) in Anspruch genommen wird, endet diese Leistung mit Erfüllung des jeweiligen Einzelauftrages.

(2) Diese Vereinbarung ist integrierender Bestandteil des Hauptvertrages und die Laufzeit entspricht der Laufzeit des jeweiligen Hauptvertrages, der zwischen den Parteien besteht.

4. Ort der Verarbeitung

Die Tätigkeit des Auftragsverarbeiters erfolgt in der Europäischen Union, in einem Staat mit angemessenem Schutzniveau oder in 574364 d einem Staat, in dem ein Sub-Auftragsverarbeiter seinen Sitz außerhalb dieser Staaten hat, ausschließlich auf Basis von ausreichenden Standarddatenschutzklauseln. Auf Aufforderung wird der Auftragsverarbeiter dem Verantwortlichen diesen Abschluss von Standarddatenschutzklauseln nachweisen.

5. Art der Verarbeitung

Die Art der Verarbeitung erfolgt nach den Regelungen des Hauptvertrages.

6. Rechtmäßigkeit der Datenverarbeitung sowie Informationspflicht

(1) Der Verantwortliche nimmt zur Kenntnis, dass es ihm obliegt, für die ausreichende Rechtsgrundlage iSd Art 6 (1) DSGVO oder Art 9 (2) DSGVO zu sorgen. Der Auftragsverarbeiter ist nicht in der Lage die Rechtsgrundlage der Verarbeitung zu prüfen.

(2) Der Verantwortliche nimmt zur Kenntnis, dass ihm die Verpflichtung obliegt, die betroffenen Personen zum Zeitpunkt der Erhebung iSd Art 13 DSGVO oder bei der indirekten Datenerhebung iSd Art 14 DSGVO rechtzeitig zu informieren. Der Verantwortliche nimmt zur Kenntnis, dass der Auftragsverarbeiter ein Empfänger der personenbezogenen Daten, und daher gegenüber den betroffenen Personen zu nennen ist (Art 13 Abs 1 lit e DSGVO; Art 14 Abs 1 lit e DSGVO).

7. Art der personenbezogenen Daten

Es werden diejenigen Datenkategorien verarbeitet, die der Verantwortliche im Rahmen des Hauptvertrages selbst definiert, wobei es sich um folgende Kategorien handelt:

Allgemeine Personendaten, Kontaktdaten, Kommunikationsdaten, Daten über die Legitimation, Berufs- und Arbeitgeberdaten, Daten von Familien- und Haushaltsangehörigen, Beschreibung der Personen (körperlich), Gewohnheiten und Interessen der Personen, Gesundheitsdaten, Versicherungsvertragsdaten, Daten zum zu versichernden Risiko, Bankdaten, Ausbildungsdaten, Bonitäts- und Einkommensdaten, gescannte Dokumente und Bilddaten, Daten zum Pensionskonto und pensionsrelevante Daten.

Zusätzlich bei Nutzung von VARIASsign: Biometrische Unterschriftsdaten, Standortdaten, IP-Adressen, übermittelte Dokumente
Auf die Inhalte der übermittelten Dokumente hat ausschließlich der Verantwortliche Einfluss. Es können darin auch Art 9 Daten enthalten sein.

8. Kategorien betroffener Personen

Kategorien betroffener Personen, die verarbeitet werden, sind:
Kunden, Interessenten, Mitarbeiter, Ansprechpartner bei Versicherungs- und sonstigen Gesellschaften und alle vom Verantwortlichen selbst definierten Personen

9. Wechselseitige Rechte und Pflichten der Vertragsparteien

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, dass er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet. Dies umfasst auch Weisungen zur Einschränkung, Berichtigung oder Löschung der Daten. Der Verantwortliche hat im Rahmen der Vertragsbeziehungen die Möglichkeit über die Software direkt die Zugriffe auf die personenbezogenen Daten selbst zu gestalten.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung von Weisungen solange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Offensichtlich rechtswidrige Weisungen werden vom Auftragsverarbeiter abgelehnt.

(3) Nach Möglichkeit unterstützt der Auftragsverarbeiter den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen (Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch und Schutz vor automatisierter Entscheidung). Wenn eine betroffene Person einen Antrag an den Auftragsverarbeiter stellen sollte, so leitet dieser den Antrag dem Verantwortlichen weiter.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung), in dem er in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestaltet, dass sie den Anforderungen des Datenschutzes gerecht wird. So wird ein angemessener Schutz der personenbezogenen Daten hergestellt. Eine Änderung der technischen und organisatorischen Maßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wenn sich durch die Änderung das Niveau des Schutzes und der Sicherung nicht verringert. Sofern aus individuellen Anfragen des Verantwortlichen, dem Auftragsverarbeiter Aufwendungen und Kosten entstehen, trägt diese der Verantwortliche.

(5) Nach Aufforderung durch den Verantwortlichen, stellt der Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DSGVO („Auftragsverarbeitung") enthaltenen Pflichten zur Verfügung. Der Auftragsverarbeiter ermöglicht auch Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem von ihr beauftragten Dritten durchgeführt werden, sofern es sich beim Dritten oder Verantwortlichen selbst nicht um einen Mitbewerber des Auftragsverarbeiters handelt. Der Verantwortliche oder der beauftragte Dritte wird bei den Prüfungen Rücksicht auf die Abläufe des Auftragsverarbeiters nehmen, und dafür Sorge tragen, dass die betrieblichen Abläufe des Auftragsverarbeiters so minimal wie möglich beeinträchtigt werden. Etwaige dem daraus Auftragsverarbeiter daraus entstehende Aufwendungen und Kosten trägt der Verantwortliche.

(7) Der Auftragsverarbeiter behandelt, die übermittelten oder sonst zur Verfügung gestellten personenbezogenen Daten und Informationen sowie die Kenntnisse über und im Zusammenhang mit der Verarbeitungstätigkeit vertraulich.

(8) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten oder tätigen Personen ist es untersagt, personenbezogene Daten des Verantwortlichen unbefugt zu erheben, zu verarbeiten oder zu nutzen.

(9) Bei Störungen, Verdacht auf Verletzungen der Vertraulichkeit, Datenverlust, Datenbeschädigung oder eine sonstige Verletzung des Datenschutzes, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Verantwortlichen, durch den Auftragsverarbeiter, bei diesen tätigen Personen oder durch Sub-Auftragsverarbeiter wird der Auftragsverarbeiter den Verantwortlichen informieren.

(10) Der Auftragsverarbeiter wird den Verantwortlichen bei Prüfungen durch die Aufsichtsbehörde (Datenschutzbehörde) informieren, sofern durch die Prüfungen die Daten des Verantwortlichen betroffen sind.

10. Verpflichtung zur Vertraulichkeit

(1) Alle dem Auftragsverarbeiter zurechenbare Personen (insb. Beschäftigte), die mit der Verarbeitung personenbezogener Daten befasst sind, sind vertraglich zur Geheimhaltung und Vertraulichkeit der Ihnen berufsmäßig bekanntgewordenen und bekanntwerdenden Daten, sowie zur redlichen Verarbeitung dieser Daten nach Treu und Glauben zu verpflichten. Auf Aufforderung durch den Verantwortlichen ist dies nachzuweisen.

(2) Darüber hinaus sind alle vom Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragten Personen dazu verpflichtet, diese Daten nur aufgrund von Anordnungen zu übermitteln. Des Weiteren sind diese Personen über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu unterrichten.

11. Sub-Auftragsverarbeitung und Verarbeitung aufgrund von Rechtsvorschriften

(1) Sämtliche Verarbeitungen werden in direkter Vertragsbeziehung des Verantwortlichen mit dem Auftragsverarbeiter durchgeführt.

(2) Es werden die in Anlage ./1 genannten Sub-Auftragsverarbeiter zur Leistungserbringung herangezogen.

(3) Der Auftragsverarbeiter ist berechtigt, Sub-Auftragsverarbeiter hinzuzuziehen, wenn dies zur Optimierung der Abläufe, insb. im Zusammenhang mit dem technologischen Fortschritt, dient. Über eine solche Hinzuziehung ist dem Verantwortlichen vorab so rechtzeitig zu verständigen, dass dagegen Widerspruch erhoben werden kann. Erfolgt binnen 5 Tagen nach der Mitteilung kein Widerspruch, dann gilt die Zuziehung des Sub-Auftragsverarbeiters zulässig. Wenn ein Widerspruch durch einen Verantwortlichen erfolgt, und der Auftragsverarbeiter hat keine Möglichkeit, die Leistung des Sub-Auftragsverarbeiters durch eine inhaltlich und aufwandsbezogen gleichartige Leistung eines anderen Sub-Auftragsverarbeiters zu substituieren, dann berechtigt ein Einspruch den Auftragsverarbeiter zur einseitigen, sofortigen Auflösung des Auftragsverarbeitungsvertrages und Hauptvertrages. Eine Liste der bei Vertragsabschluss bestehenden Sub-Auftragsverhältnisse liegt dieser Vereinbarung als Beilage bei.

(4) Der Auftragsverarbeiter schließt mit den Sub-Auftragsverarbeitern Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO. Dabei wird sichergestellt, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, welche dem Auftragsverarbeiter aufgrund dieser Vereinbarung obliegen.

(5) Dem Auftragsverarbeiter sind keine Rechtsvorschriften bekannt, welche eine andere als die hier dokumentierten Verarbeitungen erfordern würden.

(6) Ein Sub-Auftragsverarbeiterverhältnis liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen betraut, die Nebenleistungen darstellen, z.B. Post-, Transport- und Versanddienstleistungen, Reinigungsarbeiten, Telekommunikationsdienstleistungen ohne konkreten Bezug zu den personenbezogenen Daten der Verantwortlichen, Bewachungs- und Sicherheitsdienstleistungen.

12. technische und organisatorische Maßnahme sowie Verzeichnis

(1) Der Auftragsverarbeiter trifft umfassende angemessene technische und organisatorische Maßnahmen und weist diese unserer Organisation auf Aufforderung nach.

(2) Diese technischen und organisatorischen Maßnahmen werden vom Auftragsverarbeiter jeweils an den Stand der Technik angepasst.

(3) Der Auftragsverarbeiter führt ein Verarbeitungsverzeichnis gemäß Artikel 30 DSGVO.

13. Löschung bzw. Herausgabe nach Vertragsbeendigung

(1) Der Auftragsverarbeiter wird die personenbezogenen Daten nach Beendigung des Hauptvertrages unverzüglich löschen oder auf Aufforderung unserer Organisation in einem gängigen, strukturierten und maschinenlesbaren Format zur Verfügung stellen, sofern nicht nach dem Unionsrecht oder dem Recht der Republik Österreich eine Verpflichtung zur Aufbewahrung oder Speicherung der personenbezogenen Daten besteht.

(2) Etwaige Kosten und Aufwendungen aus oder im Zusammenhang mit der Datenrückgabe des Auftragsverarbeiters trägt der Verantwortliche.

14. Allgemeines

(1) Änderungen des Vertrages bedürfen der Schriftform. Dies gilt auch für das Abgehen vom Schriftformerfordernis.

(2) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder nichtig sein oder infolge Änderung der Gesetzeslage oder durch höchstrichterliche Rechtsprechung oder auf andere Weise ganz oder teilweise unwirksam oder nichtig werden oder weist dieser Vertrag Lücken auf, so sind sich die Parteien darüber einig, dass die übrigen Bestimmungen dieses Vertrages davon unberührt und gültig bleiben. Für diesen Fall verpflichten sich die Vertragsparteien, unter Berücksichtigung des Grundsatzes von Treu und Glauben an Stelle der unwirksamen Bestimmung eine wirksame Bestimmung zu vereinbaren, welche dem Sinn und Zweck der unwirksamen Bestimmung möglichst nahekommt und von der anzunehmen ist, dass die Parteien sie im Zeitpunkt des Vertragsschlusses vereinbart hätten, wenn sie die Unwirksamkeit oder Nichtigkeit gekannt oder vorhergesehen hätten. Entsprechendes gilt, falls dieser Vertrag eine Lücke enthalten sollte.

(3) Ausschließlicher Gerichtsstand für etwaige Streitigkeiten aus oder in Zusammenhang mit diesem Vertrag ist das für den Sitz des Auftragsverarbeiters sachlich zuständige Gericht.

Anlagen:
./1 Liste der Sub-Auftragsverarbeiter
./2 Beschreibung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters bzw. Subauftragsverarbeiter

Anlage 1

Liste der Sub-Auftragauftragsverarbeiter

Internex gmbH, 3950 Gmünd, Lagerstraße 15 Funktion: Managed Serverhousing und Serverhosting SEIMO Mobile Marketing GmbH, Marienstraße 13, 4020 Linz Funktion: Newslettersytem

GTX GmbH, Stresemannstraße 6, 21335 Lüneburg, Deutschland

SMS-Provider

Anlage 2
Technische und organisatorische Maßnahmen nach Art. 32 EU-DSGVO

1. Zutrittskontrolle

Maßnahmen um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Rechenzentren erhalten, in welchen personenbezogene Daten verarbeitet werden.

Gebäudesicherung

- Gebäude- und Infrastruktur Monitoring
- Videoüberwachung
- Automatisches Zutrittskontrollsystem
- Absicherung von Gebäudeschächten außerhalb der Perimeter Abgrenzung
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal und Wachpersonal
- Schriftliche Zutrittsregelungen

Sicherung der Räume

- Biometrische Zutrittskontrolle zum Rechenzentrumsbereich
- Zutrittskarte für den Zutritt zu einem Rechenzentrumsraum

2. Zugangskontrolle

Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

Zugang zu den Serversystemen (Authentifizierung)

- Server-Passwörter und Zugänge werden dem Verantwortlichen bei der erstmaligen Inbetriebnahme übergeben. Der Verantwortliche ändert die Passwörter selbstständig sofort nach der Übernahme und wählt ein komplexes Passwort unter Berücksichtigung allgemeingültiger Standards.
- Der Verantwortliche verwaltet die Zugangsdaten selbstständig und ist für deren Sicherheit und periodische Änderungen verantwortlich.

3. Zugriffskontrolle

Maßnahmen für berechtigte Administratoren zur Benutzung von internen Serversystemen zur Verwaltung.

- Berechtigungskonzept inkl. Rollendefinition
- Passwortpolicy (Mindestlänge, Sonderzeichen)
- Social Engineering Prevention

Die Verantwortung der Zugriffskontrolle von Kundensystemen obliegt dem Verantwortlichen.

4. Weitergabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der beauftragten Leistung des Hauptauftrages zur Verfügung gestellt.
- Alle Mitarbeiter sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

5. Eingabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Maßnahmen bei internen Serversystemen um sicherzustellen, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

- Protokollierung der Userlogins
- Benutzeridentifikation

Auf Kundensystemen oder Serversystemen des Verantwortlichen obliegt die Verantwortung der Eingabekontrolle des Verantwortlichen.

6. Auftragskontrolle (Art. 32 Abs. 1 lit. d DSGVO)
Maßnahmen, dass personenbezogene Daten gemäß den Weisungen des Verantwortlichen verarbeitet werden.

- Definition der Weisungsbefugnisse lt. Kundenanforderung
- Auftragsannahme nur in Schriftform oder von autorisierten Personen

7. Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Maßnahmen bei internen Serversystemen zur Verwaltung um sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

- Brandschutzmaßnahmen
- Überspannungsschutz
- Unterbrechungsfreie Stromversorgung
- Klimaanlage (Redundantes System)
- Luftfeuchtigkeit zwischen 40% und 60%
- 24/7 Monitoring der Serversysteme
- Separate Brandabschnitte
- Backupkonzept für interne Serversysteme zur Verwaltung

Auf Kundensysteme oder Serversystemen des Verantwortlichen obliegt die Verantwortung der Verfügbarkeitskontrolle, insbesondere der Datensicherung, dem Verantwortlichen, falls dies nicht schriftlich im Hauptvertrag anders vereinbart wurde.

8. Trennungsgebot

Maßnahmen, dass personenbezogene Daten auf internen Serversystemen, getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testsystemen
- Festlegung von Datenbankrechten, logische Mandantentrennung (softwareseitig)

Die Trennungskontrolle bei Kundenservern oder Serversystemen des Verantwortlichen obliegt dem Verantwortlichen.

9. Abgrenzung
Abgrenzung bei unsachgemäßer Handhabung der Software durch den Kunden. Insbesondere gilt dies bei folgenden Vorgängen:

- Datendiebstahl, welcher durch unachtsamen Umgang des Verantwortlichen mit Zugangsdaten oder mit sonstigen sicherheitsrelevanten Schutzmechanismen möglich wurde
- Unbefugter Zugriff, welcher durch unachtsames Vorgehen vom Verantwortlichen oder von einem vom Verantwortlichen dazu berechtigten Unternehmen ermöglicht wurde

- Für die Datenverarbeitung, Datensicherheit und Einhaltung der gesetzlichen Vorschriften auf Applikationsebene (z.B.: Website, Webanwendung, App, …) ist der Verantwortlichen verantwortlich
- Vom Verantwortlichen nicht autorisierte Veränderungen an Dateien oder Datenbanken, welche von einem berechtigten Unternehmen selbstständig durchgeführt wurden