

Ergänzung zum Hauptvertrag und den Allgemeinen Geschäftsbedingungen für Software-as-a-Service

Vereinbarung

zwischen

.....
- *Verantwortlicher - nachstehend Kunde (=Auftraggeber) genannt -*

und der

hyperspace GmbH, Plaggestraße 24, 26419 Schortens

- *Auftragsverarbeiter - nachstehend Auftragnehmer genannt*

Präambel

Der Auftragnehmer stellt dem Kunden gemäß den "Allgemeine Geschäftsbedingungen für Software-as-a-Service (SaaS) - Stand Mai 2018" ("AGB SaaS") sowie der zugehörigen Service-Bedingungen (gemeinsam "Hauptvertrag") ihre Softwareprodukte ("Software") zur Nutzung über das Internet zur Verfügung. Die Software wird vom Auftragnehmer in einem Rechenzentrum betrieben und dem Kunden zur Nutzung über das Internet zur Verfügung gestellt (auch als "Software as a Service" Modell bezeichnet).

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen den Vertragsparteien bestehenden Verträgen, Vereinbarungen, oder seitens des Auftraggebers erteilten Aufträgen an den Auftragnehmer zur Bereitstellung von Dienstleistungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

Dabei steht die Verarbeitung von personenbezogenen Daten nicht im Fokus der eigentlichen Leistungserbringung der hyperspace GmbH. Durch die erbrachten Dienstleistungen kann jedoch der Zugriff auf personenbezogene Daten des Kunden durch den Auftragnehmer, z.B. im Zuge von Wartungsarbeiten oder Fehlerbehebungen, nicht ausgeschlossen werden. Darüber hinaus können implizit im Rahmen einer Leistungserbringung personenbezogene Daten des Kunden verarbeitet werden, z.B. im Rahmen eines durch den Auftragnehmer bereitgestellten Datensicherungsprozesses.

Die folgende Vereinbarung regelt den Umgang mit entsprechenden Daten.

1. Gegenstand, Dauer und Beschreibung der Auftragsverarbeitung

Verarbeitung personenbezogener Daten

Diese Vereinbarung ("Vertrag") regelt die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, die (i) der Auftraggeber bzw. deren Benutzer im Rahmen der Verwendung der Software in diese eingibt, (ii) die mit der Nutzung der Software entstehen oder sonst erhoben werden, und (iii) die der Kunde im Zusammenhang mit der Durchführung des Hauptvertrages dem Auftragnehmer in sonstiger Weise überlässt ("Daten"). Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person.

Inhalt der Auftragsverarbeitung

Soweit es sich bei den Kundendaten um personenbezogene Daten handelt, verarbeitet die hyperspace GmbH die Kundendaten als Auftragsverarbeiter im Sinne von Art. 28 DSGVO ausschließlich im Auftrag und nach den Weisungen des Kunden und ausschließlich zum Zwecke der Bereitstellung des Services. Der Kunde bleibt alleiniger Eigentümer seiner Daten. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedsstaat 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 Art. 44 ff. DS-GVO erfüllt sind.

Hyperspace stellt dem Kunden Softwareprodukte zur Nutzung über das Internet zur Verfügung ("Software as a Service").

Im Zuge von Wartungs- und Einrichtungsarbeiten, Einspielen von Softwareupdates, Durchführung von Backups oder Restores oder Durchführung von Fehlerdiagnosen kann ein Zugriff auf personenbezogene Daten des Kundensystems nicht ausgeschlossen werden.

In allen Fällen gilt, dass hyperspace eine bewusste Einsichtnahme, Anfertigung einer Kopie, Veränderung, Löschung oder anderweitige Bearbeitung der personenbezogenen Daten ohne vorherige explizite Weisung oder außerhalb des Rahmens der beschriebenen Leistungen durch den Kunden untersagt ist.

Art der Daten

Im Rahmen der oben aufgeführten Leistungen ist nicht ausgeschlossen, dass hyperspace Zugriff auf folgende Daten oder Datenarten haben kann:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Profil- oder Avatarbilder von Benutzern
- Termine und Aufgaben von Benutzern
- Berechtigungen und Verantwortlichkeiten von Benutzern
- Zeitpunkte des Logins von Benutzern
- Protokolldaten über das Anlegen, Ändern und Löschen von Objekten durch Benutzer
- Planungs- und Steuerungsdaten

- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Bei Nutzung des Schulungsmanagement-Moduls: Anwesenheitslisten, Teilnehmerlisten, Beurteilungen, Kursinfos, Qualifizierungen und Zeugnisse von Schulungsteilnehmern sowie Qualifizierungen und Historie der durchgeführten Schulungsmaßnahmen von Dozenten
- bei Nutzung des CRM-Moduls: Firmenname, Firmenadresse, E-Mail, Telefon, Fax, Website-URL; Personen-Name, Vorname, Anredeform, Personen-Adresse, Personen-E-Mail, Telefonnummern, URLs von Profildaten in sozialen Medien, Geburtsdatum, Kategorie (z.B. Lieferant, Kunde), Ursprung, Funktion (z.B. Abteilungsleiter), Stammdaten, Identifikationsdaten, Kommunikationsdaten, Termine, Angebotsdaten, Historie, Informationen über Waren und Dienstleistungen; Bilder; ggf. weitere persönliche oder beschreibende Informationen
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten

Betroffene Personenkreise

- Kunden
- Interessenten
- Benutzer
- Beschäftigte / Mitarbeiter
- Bewerber
- Lieferanten / Geschäftspartner
- Handelsvertreter
- Ansprechpartner
- Teilnehmer an Schulungen
- Dozenten für Schulungen

2. Anwendungsbereich und Verantwortlichkeiten

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich («Verantwortlicher» im Sinne des Art. 4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

3. Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein

Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. 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 solange 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. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
3. Datenschutzbeauftragter: Als externer Datenschutzbeauftragter für hyperspace ist seit dem 01.07.2017 die René Rautenberg GmbH, Hauptstrasse 28, 15806 Zossen bestellt. E-Mail: datenschutzbeauftragter@hyperspace.de
4. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
5. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. (Anmerkung: Im Hauptvertrag können die Parteien hierzu eine Vergütungsregelung treffen).
6. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter 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.
7. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
8. 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.
9. Ansprechpartner beim Auftragnehmer für im Rahmen des Vertrages anfallende Datenschutzfragen ist Ralf Guttmann, Geschäftsführer der hyperspace GmbH. Anfragen sind per E-Mail zu richten an: datenschutzbeauftragter@hyperspace.de

10. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
11. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Hauptvertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag bereits vereinbart.
12. Daten, exklusiv genutzte Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.
13. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

4. Pflichten des Auftraggebers

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 13 entsprechend.
3. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Als Ansprechpartner zum Zeitpunkt des Vertragsabschlusses wird benannt:

Vorname

Name

E-Mail

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. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder durch einen von Auftraggeber beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf Inspektion von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, kann der Auftragnehmer eine Inspektion durch diesen Prüfer ablehnen. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

7. Subunternehmer (weitere Auftragsverarbeiter)

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. 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 ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
3. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung, dass diese Unterauftragsverhältnisse durch angemessene

vertragliche Vereinbarungen sowie Kontrollmaßnahmen gemäß DSGVO ausgestaltet wurden und ein gesetzskonformes Datenschutzniveau gewährleistet wird:

Unterauftragnehmer	Anschrift inkl. Land	Leistung
Hostway Deutschland GmbH,	Am Mittelfelde 29, 30519 Hannover, Deutschland	Rechenzentrumsbetrieb / Technischer Betrieb der hyperspace Server und Internetkonnektivität
CompuTron GNetX Daniel Lindstedt	Hirsauerstr. 224, 75180 Pforzheim, Deutschland	Email-To-Fax-Gateway
Esendex Limited	15 Warwick Road, Startford Upon Avon, CV37 6YW, England	Email-To-SMS-Gateway

8 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers 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 Anlage 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 Anlage zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Es gilt deutsches Recht.

9 Haftung und Schadensersatz

Eine zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

Für den Auftraggeber (Kunde):	Für den Auftragnehmer (hyperspace GmbH):
Name (in Blockbuchstaben)	Ralf Guttman Name (in Blockbuchstaben)
Position / Funktion	Geschäftsführer Position / Funktion
Ort, Datum	Schortens, 22. Mai 2018 Ort, Datum
Unterschrift und Stempel	 Unterschrift und Stempel  Plaggestr. 24 · D-26419 Schortens Telefon: +49 (0) 44 61 - 9 16 00 05 Telefax: +49 (0) 44 61 - 9 16 00 08 Internet: www.hyperspace.de Mail: info@hyperspace.de

ANHANG: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Hyperspace kann im Rahmen der Leistungserbringung mit personenbezogenen Daten in Kontakt kommen. Dabei steht die Verarbeitung von personenbezogenen Daten nicht im Fokus der eigentlichen Leistungserbringung von hyperspace. Durch die erbrachten Dienstleistungen kann jedoch der technische Zugriff auf personenbezogene Daten des Kunden durch hyperspace nicht ausgeschlossen werden. Gemäß Artikel 32 DSGVO hat hyperspace technische und organisatorische Maßnahmen zu treffen, wann immer personenbezogene Daten verarbeitet werden. Diese sind erforderlich um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

hyperspace erfüllt diesen Anspruch durch die im Folgenden dokumentierten Maßnahmen:

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

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Sicherheitsschlösser
- Sicherheitsbeschläge
- Einbruchhemmende Fenster
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Keine unbefugte Systembenutzung:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe nach sicheren Kennwortrichtlinien
- Authentifikation mit Benutzername / Passwort

- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- IT-Sicherheitsrichtlinie für die Nutzung externer Schnittstellen (USB etc.)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz von Hardware-Firewall
- Einsatz von Software-Firewalls bei allen Arbeitsplätzen

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Protokollierung von Fernwartungsarbeiten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystemen

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

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Remote-Zugriff mittels verschlüsselter Verbindung
- Nutzung von VPN-Tunneln

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

- Unterbrechungsfreie Stromversorgung (USV)
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

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

Datenschutz-Management

- Datenschutz Management mit dem ER Secure Management System

IT Störungsmanagement

- Notfallplan wurde erstellt

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

- Berechtigungskonzept
- Möglichkeit der Datenportabilität
- Lösbarkeit von Daten
- Protokollierung von Eingabe, Änderung, Löschung von Daten

Auftragskontrolle

- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte wurden vereinbart
- Regelmäßige Kontrollen über die Einhaltung des Datenschutzes beim Auftragnehmer werden durchgeführt

(Ende des Dokumentes)