Vertrag zur Auftragsverarbeitung bzgl. des Webhostings mit HostPress

zwischen dem / der

_____

_____

_____

- Auftraggeber, nachstehend Verantwortlicher genannt -

und

HostPress GmbH, Bahnhofstr. 34, 66571 Eppelborn

- Auftragnehmer, nachstehend genannt HOSTPRESS -

zusammen auch – die Parteien – genannt

Präambel

HOSTPRESS betreibt mit dem Service HostPress.de einen Hosting-Dienst, mit dem schnell und einfach Internetseiten mit dem Content-Management-System WordPress betrieben werden können und der von HOSTPRESS unter Nutzung von externen Rechenzentren der in diesem Vertrag genannten Unterauftragnehmer zur Verfügung gestellt wird. Je nach gebuchtem Plan übernimmt HOSTPRESS dabei nicht nur das Hosting, sondern auch das Management inkl. dem Einspielen von Updates wie die Optimierung der jeweiligen WordPress-Installation des Verantwortlichen. Weitergehender Support kann hinzugebucht werden. Im Rahmen der damit verbundenen Tätigkeiten kann nicht ausgeschlossen werden, dass HOSTPRESS in diesem Zusammenhang personenbezogene Daten für den Verantwortlichen verarbeitet.

Grundlage dieser Datenverarbeitung ist der HostPress-Hosting-Vertrag, der zwischen den Parteien abgeschlossen wurde. Dieser Vertrag zur Auftragsverarbeitung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien aus Art. 28 DSGVO sowie dem Hauptvertrag und findet Anwendung auf alle Tätigkeiten von HOSTPRESS, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte von HOSTPRESS oder durch HOSTPRESS Beauftragte mit personenbezogenen Daten des Verantwortlichen und/oder der Kunden des Verantwortlichen und/oder der Partner des Verantwortlichen und/oder anderer Betroffener in Berührung kommen könnten.

Dieser Vertrag entspricht den Anforderungen an einen Vertrag über die Auftragsverarbeitung nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG-neu) sowie den Vorschriften der Datenschutz-Grundverordnung (DSGVO). Die in diesem Vertrag verwendeten datenschutzrechtlichen Rechtsbegriffe orientieren sich an den in der DSGVO verwendeten Begriffen.

Entsprechend den gesetzlichen Vorschriften über die Auftragsverarbeitung werden die folgenden Punkte geregelt:

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1. Der Gegenstand und die Dauer der Auftragsverarbeitung (nachfolgend: Auftrag) zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ergeben sich aus dem Hauptvertrag. Gegenstand des Auftrags ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch HOSTPRESS für den Verantwortlichen. Im Zuge der Leistungserbringung von HOSTPRESS als IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Serversystemen des Verantwortlichen, kann ein Zugriff auf personenbezogene Daten auf den WordPress-Installationen des Verantwortlichen jedoch nicht ausgeschlossen werden.

1.2. Die Laufzeit dieses Auftrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Auftrags nicht darüber hinausgehende Verpflichtungen ergeben.

1.3. Art der Daten:

Zum Zwecke der Vertragserfüllung des Hauptvertrages kann ein Zugriff von HOSTPRESS

- ⇨ beim Hosting von Server-Systemen und dort betrieben Anwendungen (Datenbank-,Backup-, Web-Server, SAN-Umgebung),
- ⇨ bei der technischen Administration der Server-Systeme, inkl. der Installation von Plugins oder Arbeiten an den Datenbanken, die von den WordPress-Instanzen des Verantwortlichen genutzt werden,

- ⇨ bei sonstigen Support-Tätigkeiten für sämtliche Server-Systeme (z.B. im Rahmen des proaktiven Monitorings),
- ⇨ im Rahmen der Auswertung von Log-Files,

auf alle Daten des Verantwortlichen und seiner Kunden, die der Verantwortliche innerhalb der HostPress-Instanz verarbeitet, nicht ausgeschlossen werden, z.B.:

- ⇨ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ⇨ Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ⇨ Kundendaten (z.B. Name, Geburtsdatum, Anschrift)
- ⇨ Mitarbeiterdaten (z.B. Name)
- ⇨ Vertragsabrechnungs- und Zahlungsdaten
- ⇨ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ⇨ Alle sonstigen Daten, die der Verantwortliche in der HostPress-Umgebung verarbeitet.

1.4. Kreis der Betroffenen:

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst alle Personen, deren Daten von dem Verantwortlichen mit der HostPress-Instanz verarbeitet werden, z.B.:

- ⇨ Kunden
- ⇨ Interessenten
- ⇨ Beschäftigte (z.B. Arbeitnehmer, Bewerber)
- ⇨ Lieferanten
- ⇨ Handelsvertreter
- ⇨ Ansprechpartner
- ⇨ Alle sonstigen Personen, deren Daten von dem Verantwortlichen mittels der HostPress-Umgebung verarbeitet werden.

1.5. HOSTPRESS hostet den Service HostPress in deutschen Rechenzentren der Firmen Gridscale GmbH, Hetzner Online GmbH und Krämer IT Solutions GmbH (nachfolgend gemeinsam: SERVERANBIETER).

1.6. Die SERVERANBIETER organisieren die Sicherheit des jeweiligen Rechenzentrums selbst und werden diesbezüglich als Unterauftragsverarbeiter gemäß Ziffer 6 dieses Vertrags für HOSTPRESS tätig.

1.7. Hierfür wurde jeweils ein Vertrag zur Auftragsverarbeitung zwischen HOSTPRESS und den SERVERANBIETERN abgeschlossen. HOSTPRESS gewährleistet, dass dem Verantwortlichen die Rechte aus diesen Verträgen zur Auftragsverarbeitung mit den SERVERANBIETERN in gleichem Umfang zustehen. Im Fall widersprüchlicher Regelungen zwischen diesem Auftragsverarbeitungsvertrag und den Verträgen zur Auftragsverarbeitung mit den SERVERANBIETERN haben die vertraglichen Regeln aus diesem Auftragsverarbeitungsvertrag Vorrang.

1.8. Neben dem HostPress-Dienst findet eine Datenverarbeitung der betroffenen Daten am Standort von HOSTPRESS in Eppelborn nicht statt. Ein Zugriff durch HOSTPRESS auf die innerhalb von HostPress gespeicherten Daten ist nur mittels einer verschlüsselten Verbindung möglich. Details hierzu ergeben sich aus den technischen und organisatorischen Maßnahmen in Anlage 1 dieses Vertrages.

2. Anwendungsbereich und Verantwortlichkeit, Haftungsfreistellung

2.1. HOSTPRESS verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dies umfasst Tätigkeiten, die im Hauptvertrag und im Auftrag konkretisiert sind. Der Verantwortliche ist im Rahmen dieses Auftrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an HOSTPRESS sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO), soweit nicht das anwendbare Datenschutzrecht ausdrücklich eine eigenständige Verantwortlichkeit oder Haftung von HOSTPRESS vorsieht; für die Einhaltung solcher Bestimmungen bleibt HOSTPRESS (ggf. neben dem Verantwortlichen) verantwortlich.

2.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2.3. Soweit HOSTPRESS gemäß den Weisungen des Verantwortlichen handelt und die technischen und organisatorischen Maßnahmen und die sonstigen ihm durch diese Vereinbarung auferlegten Verpflichtungen beachtet, stellt der Verantwortliche HOSTPRESS auf erstes Anfordern von allen rechtlichen Ansprüchen, Schäden und Kosten frei, soweit diese dadurch entstehen, dass Dritte oder betroffene Personen aus der Datenverarbeitung resultierende Ansprüche gegen HOSTPRESS geltend machen. Hiervon umfasst sind insbesondere auch die

Kosten der notwendigen Rechtsverteidigung einschließlich sämtlicher Gerichts- und Anwaltskosten in der jeweiligen gesetzlichen Höhe, sowie Bußgelder in tatsächlich festgesetzter Höhe in dem Umfang, in dem der Verantwortliche Anteil an der Verantwortung für den durch das Bußgeld sanktionierten Verstoß trägt. Gegenstand der Freistellung sind demnach insbesondere Ansprüche aufgrund von rechtswidrigen Weisungen des Verantwortlichen gemäß Art. 28 Abs. 3 S. 3 DSGVO sowie nicht ausreichender technisch-organisatorischer Maßnahmen, die gemäß Ziffer 3 dieser Vereinbarung vom Verantwortlichen freigegeben wurden. Dem Verantwortlichen bleibt im Nachgang vorbehalten, nachzuweisen, dass die gegen HOSTPRESS gerichteten, vorgenannten Ansprüche und Bußgelder nicht auf Weisungen oder Pflichtverletzungen des Verantwortlichen beruhen.

3. Technisch-organisatorische Maßnahmen

3.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und HOSTPRESS geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.2. HOSTPRESS hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen zu prüfen und HOSTPRESS Änderungswünsche mitzuteilen. HOSTPRESS ist berechtigt, Änderungswünsche abzulehnen und/oder unter den Vorbehalt der Kostenübernahme durch den Verantwortlichen zu stellen. Soweit die technischen und organisatorischen Maßnahmen gem. Anlage 1 von dem Verantwortlichen akzeptiert werden, werden diese ausschließliche Grundlage des Auftrages i.S.d. Ziffer 2.12.3. Soweit die Prüfung des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3. Der Verantwortliche ist im Rahmen dieser Vereinbarung allein verantwortlich für die Beurteilung der Angemessenheit der technischen und organisatorischen Maßnahmen. HOSTPRESS setzt die vom Verantwortlichen geprüften Maßnahmen entsprechend dem gemäß Ziffer 3.2 dokumentierten Umfang um.

3.4. Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen, die den angemessenen Schutz der personenbezogenen Daten des Verantwortlichen sicher stellen sollen und die den Anforderungen der DSGVO (Art. 32) genügen. Diese Maßnahmen werden wie folgt festgelegt, sind entsprechend zu dokumentieren und dem Verantwortlichen vorzulegen: Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie die Einhaltung des Trennungsgebots. Darüber hinaus sind auch auftragsspezifische Maßnahmen umzusetzen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand. Die Maßnahmen schließen unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.5. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es HOSTPRESS gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3.6. Der Verantwortliche und HOSTPRESS unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. Anfragen Betroffener, Berichtigung, Sperrung und Löschung von Daten; Unterstützung durch HOSTPRESS

4.1. HOSTPRESS hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an HOSTPRESS zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird HOSTPRESS dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Die Prüfung der Anfrage obliegt ausschließlich dem Verantwortlichen.

4.2. HOSTPRESS verpflichtet sich, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in Ansehung der Art der Verarbeitung dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der Datenschutzgrundverordnung genannten Rechte der betroffenen Person nachzukommen.

4.3. Ist der Verantwortliche auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, oder ist der Verantwortliche zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder zur Datenübertragung verpflichtet, wird HOSTPRESS den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen

Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung dieser Rechte nachzukommen.

4.4. Der Verantwortliche wird HOSTPRESS schriftlich oder in einem dokumentierten elektronischen Format zur Mitwirkung auffordern, sofern solche Mitwirkungshandlungen von HOSTPRESS erforderlich sind. Der Verantwortliche stellt HOSTPRESS auf erste Anforderung von den durch diese Unterstützung entstandenen Kosten frei, soweit HOSTPRESS dem Verantwortlichen vorab den Kostenrahmen schriftlich oder in Textform mitgeteilt hat.

4.5. HOSTPRESS wird keine Auskunftsverlangen oder anderweitige Anfragen bezüglich der Rechte Betroffener beantworten und den Betroffenen insoweit an den Verantwortlichen verweisen.

4.6. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an HOSTPRESS, wird HOSTPRESS den Betroffenen an den Verantwortlichen verweisen.

4.7. Die Parteien werden für alle vorstehenden Tätigkeiten – soweit sie keiner gesetzlichen Verpflichtung entsprechen - ein angemessenes Entgelt vereinbaren, soweit erkennbar wird, dass hierfür der Aufwand von HOSTPRESS das übliche Maß überschreitet.

5. Kontrollen und sonstige Pflichten von HOSTPRESS

HOSTPRESS hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

- ⇨ Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 bis 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- ⇨ HOSTPRESS gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet HOSTPRESS, 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.
- ⇨ Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO.
- ⇨ Unterstützung des Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der HOSTPRESS zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit der Verarbeitung (z.B. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Durchführung einer Datenschutz-Folgenabschätzung oder der vorherigen Konsultation der Aufsichtsbehörde). HOSTPRESS wird diese unterstützenden Tätigkeiten – soweit sie keiner gesetzlichen Verpflichtung entsprechen – nur gegen ein angemessenes Entgelt durchführen. Die Parteien werden im Einzelfall ein entsprechendes Entgelt miteinander abstimmen.
- ⇨ Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit die Datenverarbeitungsprozesse, die von HOSTPRESS für den Verantwortlichen ausgeführt werden, betroffen sind. Dies gilt auch, soweit eine zuständige Datenschutz-Aufsichtsbehörde bei HOSTPRESS ermittelt.
- ⇨ Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch HOSTPRESS im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- ⇨ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen. Hierzu kann HOSTPRESS auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit z.B. i.S.d. Art. 40, 42 DSGVO vorlegen.
- ⇨ Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Verantwortlichen sind nicht Gegenstand der von HOSTPRESS zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

6. Unterauftragsverhältnisse

6.1. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten von HOSTPRESS Unterauftragsverarbeiter einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- ⇨ Die Einschaltung von Unterauftragsverarbeitern ist grundsätzlich nur mit schriftlicher Zustimmung des Verantwortlichen gestattet. Ohne schriftliche Zustimmung kann HOSTPRESS zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragsverarbeiter mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Verantwortlichen vor Beginn der Verarbeitung oder Nutzung mitteilt und der Verantwortliche hierdurch die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

⇨ HOSTPRESS hat die vertraglichen Vereinbarungen mit dem / den Unterauftragsverarbeiter/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Verantwortlichen und HOSTPRESS entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass sie den gesetzlichen Anforderungen des Datenschutzrechts entsprechen.

⇨ Bei der Unterbeauftragung sind Kontroll- und Überprüfungsrechte des Verantwortlichen entsprechend dieser Vereinbarung beim Unterauftragsverarbeiter einzuräumen. Dies umfasst auch das Recht des Verantwortlichen, von HOSTPRESS auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

6.2. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die HOSTPRESS bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. HOSTPRESS ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.3. HOSTPRESS wird die nachfolgend aufgeführten Unterauftragsverarbeiter zur Erfüllung seiner vertraglich geschuldeten Leistungen einsetzen:

Name des Unterauftragsverarbeiters	Gegenstand der Unterbeauftragung	Zertifikate, Mitgeltende Unterlagen
Gridscale GmbH, Im Mediapark 5, 50670 Köln	Rechenzentrumsdienstleistungen	AV-Vertrag abgeschlossen, Serverstandorte ausschließlich in Deutschland, ISO 27.001, 22.301, 20.000, 9.001
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Rechenzentrumsdienstleistungen	AV-Vertrag abgeschlossen, Serverstandorte ausschließlich in Deutschland, ISO 27.001
Krämer IT Solutions GmbH, Koßmannstr. 7, 66571 Eppelborn	Rechenzentrumsdienstleistungen	AV-Vertrag abgeschlossen. Serverstandorte ausschließlich in Deutschland

7. Kontrollrechte des Verantwortlichen

7.1. Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von HOSTPRESS und dokumentiert das Ergebnis.

⇨ Hierfür kann er z. B. Auskünfte von HOSTPRESS einholen,

⇨ sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen

⇨ oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu HOSTPRESS steht.

7.2. HOSTPRESS verpflichtet sich, dem Verantwortlichen auf Anforderung in Textform innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen und Prüfungen – einschließlich Inspektionen - , die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen oder dazu beizutragen, die zur Durchführung einer Kontrolle erforderlich sind.

8. Mitteilung bei Verstößen von HOSTPRESS

8.1. HOSTPRESS unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Verstößen von HOSTPRESS oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder die in diesem Vertrag getroffenen Festlegungen.

8.2. HOSTPRESS trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab.

8.3. HOSTPRESS unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten nach Art. 33 DSGVO.

9. Weisungsbefugnis des Verantwortlichen

9.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen in dem zu Grunde liegenden Vertrag und diesem Auftragsverarbeitungsvertrag und nach dokumentierter Weisung von dem

Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

9.2. Auskünfte an Dritte darf HOSTPRESS nur nach vorheriger schriftlicher Zustimmung des Verantwortlichen erteilen.

9.3. Der Verantwortliche wird mündliche Weisungen unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. HOSTPRESS verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen 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.

9.4. Die vorstehenden Beschränkungen der Ziffern 9.1 bis 9.3 bezüglich der Verarbeitung personenbezogener Daten gelten nur, sofern HOSTPRESS nicht durch das Recht der Union oder der Mitgliedstaaten, dem HOSTPRESS unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt HOSTPRESS dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

9.5. HOSTPRESS hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. HOSTPRESS ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

9.6. Bezüglich der Weisungsbefugnis wird Folgendes vereinbart:

Die Parteien verpflichten sich, Ansprechpartner für die Weisungen im Nachgang gesondert zu benennen. Bei Wechsel oder längerfristiger Verhinderung des jeweiligen Ansprechpartners haben die Parteien unverzüglich schriftlich oder in einem dokumentierten elektronischen Format einen Nachfolger bzw. Vertreter zu benennen, wobei die Benennung nicht zwingend namentlich zu erfolgen hat, sondern sich auf auf eine bestimmte Funktion im Unternehmen beziehen kann, z.B. den Leiter der IT-Abteilung. Mitglieder der Geschäftsführung sind stets weisungsbefugt bzw. zuständige Weisungsempfänger.

Weisungsberechtigte Personen des Verantwortlichen sind:

Name	Funktion	Telefon / E-Mail-Adresse

Weisungsempfänger bei HOSTPRESS sind:

Name	Funktion	Telefon / E-Mail-Adresse
Marcus Krämer	Geschäftsführer (CEO)	+49 6881 9999777 marcus@hostpress.de
Thomas Kleinbauer	Leiter Kundensupport	+49 6881 9999777 thomas@hostpress.de

9.7. Die Parteien verpflichten sich, bei Wechsel oder längerfristiger Verhinderung des jeweiligen Ansprechpartners unverzüglich schriftlich einen Nachfolger bzw. Vertreter gem. den Vereinbarungen in Ziffer 9.6 zu benennen.

10. Löschung von Daten und Rückgabe von Datenträgern

10.1. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Vertrages hat HOSTPRESS sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen an den Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten

10.2. Eine Löschung von Daten erfolgt aber nur sofern nicht nach dem Unionsrecht oder dem anwendbaren Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist von HOSTPRESS auf Anforderung vorzulegen.

11. Informationspflichten, Schriftformklausel, Rechtswahl

11.1. Sollten die Daten des Verantwortlichen bei HOSTPRESS durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat HOSTPRESS den Verantwortlichen unverzüglich darüber zu informieren. HOSTPRESS wird alle in

diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Verantwortlichen als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes bzw. als »Verantwortlicher« im Sinne der Datenschutzgrundverordnung liegen.

11.2. Änderungen und Ergänzungen dieses Auftrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen von HOSTPRESS – bedürfen einer schriftlichen Vereinbarung 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.

11.3. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz, ggf. bestehenden datenschutzrechtlichen Regelungen des Hauptvertrags vor. Sollten einzelne Teile dieses Auftragsverarbeitungsvertrags unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags im Übrigen nicht.

11.4. Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

11.5. Die folgende Anlage ist Vertragsbestandteil:

Anlage 1 – Technische und organisatorische Maßnahmen

Ort: _____ Datum:_____ Ort: _____ Datum:_____

HOSTPRESS Verantwortlicher

Anlage 1:

zum AV-Vertrag vom:

Technische und organisatorische Maßnahmen gem. Art.32 DSGVO

Die HostPress-Dienste basieren auf einer Serverinfrastruktur. Für diese gilt das Prinzip der geteilten Verantwortung. Hierbei sind die SERVERANBIETER für die relevanten Maßnahmen zur Sicherheit der Serverinfrastruktur als solche und HOSTPRESS für die Sicherheit der Daten innerhalb dieser Serverinfrastruktur verantwortlich. Daher verweist HOSTPRESS für die relevanten Maßnahmen zur Sicherheit der Serverinfrastruktur an die jeweiligen, im Vertrag zur Auftragsdatenverarbeitung unter Ziffer 6 genannten SERVERANBIETER.

Die Haftung von HOSTPRESS gemäß den vertraglich vereinbarten Regelungen wird durch das Prinzip der geteilten Verantwortung nicht berührt.

Die nachfolgenden TOMs beschreiben die technischen und organisatorischen Maßnahmen der HOSTPRESS am Standort Eppelborn sowie die TOMs der SERVERANBIETER jeweils unter einem eigenen Unterpunkt.

I. Technische und organisatorische Maßnahmen der HOSTPRESS am Standort Eppelborn

1. Zutrittskontrolle

Um die Zutrittskontrolle zu gewährleisten und Unbefugten den Zutritt zu Datenverarbeitungsanlagen, zu verwehren sind folgende Maßnahmen getroffen worden:

- Das Gebäude wird durch eine Alarmanlage geschützt. Die Flure werden bei aktivierter Alarmanlage durch Bewegungsmelder überwacht. Sie lösen einen lauten Alarm aus der auch direkt an mehrere Verantwortliche durch geschaltet wird.
- Sämtliche Zugänge sowie die Flur- und Treppenbereiche sind durchgehend videoüberwacht.
- Geschützte Bereiche wie Büro- & Technikräume sind nur mittels Chipkarten-/Transponder-Schließsystem für berechtigte Mitarbeiter erreichbar.
- Die Reinigung der Betriebsräume wird nur von hauseigenem Personal vorgenommen. Während der Reinigung können keine vertraulichen Unterlagen eingesehen werden.

2. Zugangskontrolle

a. Benutzer-Authentifikation

- Nur authentifizierte Benutzer haben Zugang zu den Endgeräten (Clients), über die ein Zugriff auf die Server in den Rechenzentren der SERVERANBIETER möglich ist. Zusätzlich sind diese PCs passwortgeschützt und die Daten darauf verschlüsselt.
- Der Zugang zu der Server-Infrastruktur der SERVERANBIETER erfolgt mittels einer verschlüsselten SSH-Verbindung, die durch Benutzername und Passwort abgesichert ist.

b. Serversysteme

- Die Serversysteme werden von eigenem Personal konfiguriert und gepflegt.
- Die Kennungen der Administratoren, denen besondere Eindringungstiefen zugebilligt sind werden durch Username und Passworte geschützt. Die Administratoren ändern ihre Passwörter regelmäßig.

c. Monitore

Die Monitore der Entwickler Administratoren besitzen eine Bildschirmsperre mit automatischer Aktivierung und passwortgeschützter Aufhebung.

d. Internet

- Der Zugriff auf den Application-Server ist nur mit Username und Passwort durch die berechtigten Administratoren möglich. Das Passwort wird regelmäßig geändert uns ist nur den Administratoren bekannt.
- Der Zugang zum Internet ist mit einer Firewall abgesichert.

e. Firewall

- Die Regeln der Firewall sind durch Parameter einstellbar, dafür gibt es eine eigene Administrationsoberfläche. Die Administration der Firewall erfolgt ausschließlich durch den Netzwerkadministrator. Der Zugriff auf die Firewall ist nur mit Username und Passwort durch die berechtigten Administratoren möglich. Das Passwort wird regelmäßig geändert und ist nur den Administratoren bekannt Die Firewall wird mit den neuesten Patches, Updates und Virendefinitionen aufgewertet sobald diese dem Administrator zugänglich sind; Dies kann sogar stündlich geschehen wenn es nötig ist.
- Es werden alle Zugriffsversuche, zulässige und unzulässige protokolliert und die IP-Adressen aufgezeichnet.

f. Datenbank

- Die Daten von HOSTPRESS werden ausschließlich in Datenbanken gehalten.
- Für die Datenbankverwaltung gibt es einen ausschließlich und auf Dauer beauftragten Admin. Er ist nicht nur für die Konsistenz der Datenbanken verantwortlich, sondern auch für die Zuweisung von Speicherplatz, die in Zusammenarbeit mit den Administratoren vorgenommen wird.
- Zugriff auf die Datenbanken haben ausschließlich nur die Administration und der Datenbank-Admin. Der Zugriff auf die Datenbank ist nur mit Username und Passwort durch die berechtigten Administratoren möglich.
- Jeder der Zugriffsberechtigten ändert sein Passwort in regelmäßigen Abständen.

3. Zugriffskontrolle

a. Administratoren

- Die Administratoren haben Zugriff auf das gesamte System.
- Die Administratoren genießen, wie auch in anderen Unternehmen einen hohen Vertrauensvorschuss. Ihre Verhaltensweisen werden von Selbstdisziplin und Verantwortungsbewusstsein geprägt Die berechtigten Administratoren sind hochgradig vertrauenswürdig.
- Administratoren sind genau wie System Verwalter, Netzverwalter oder Privilegien Verwalter Personen mit besonderen Zugriffsmöglichkeiten zu allen Ressourcen der Datenverarbeitung. Sie stehen immer im Spannungsfeld zwischen den Handlungen, die ihnen möglich wären, und dem, was sie tun dürfen und müssen.
- Mit der Kenntnis des Usernamens und des Passwortes eines Administrators stehen ihm alle Systemressourcen offen. Er hat eine nahezu unbeschränkte Eindringtiefe in das jeweilige System und damit auch in die Anwendungen. Damit kann er alle Anwendungspassworte, die Berechtigungstabellen, die individuellen Erlaubnisse und Verbote einsehen und auch verändern. Er kann sämtliche systemeigenen Schutzrechte umgehen und auf alles zugreifen, was möglicherweise als Verursacher eines Fehlers auftreten könnte. Er kann neue Benutzer einrichten und ihnen Erlaubnisse erteilen, vorhandene Benutzer löschen oder ihre Berechtigungen ganz oder teilweise sperren. Er kann ihre Systempassworte zwar in den meisten Systemen nicht lesen, wohl aber löschen und neue zuweisen. Alle diese Tätigkeiten muss er ausführen können, um bei Systemfehlern reagieren zu können, um aus dem System die höchstmögliche Leistung herauszuholen und um die Nutzer auf die ihnen erlaubte Ausbreitung im System einzuschränken.
- Aufgrund dieser Funktionsvielfalt ist ihm das System im oben erwähnten Umfang geöffnet und die hohe Eindringtiefe ermöglicht
- Die Administratoren haben aufgrund ihrer Funktion und selbstverständlich die Möglichkeit, alle Daten der Datenbank einzusehen oder evtl., auch zu verändern. Auf der anderen Seite sind für jemanden anderen, der sich unberechtigterweise Zugang zur Datenbank verschaffen sollte, die Hürden sehr, sehr hoch, denn er müsste außerdem den richtigen Servernamen, den richtigen Datenbank-Dateinamen und den Usernamen und das Passwort für die entsprechende Datei kennen.
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

b. User

- Das System basiert auf einer strikten Trennung zwischen der User-Schicht und der Datenbank- Schicht.
- Die Abfrage eines Kunden/Externen-Users läuft wie folgt ab:
- Login des Users mit Benutzername und Kennwort in der betreffenden (branchenspezifischen) Web-Anwendungssoftware. Der Zugriff auf die HostPress-Dienste in den Rechenzentren der SERVERANBIETER erfolgt über eine mittels HTTPS abgesicherte Weboberfläche.
- Es ist jederzeit sichergestellt, dass der Kunden nur seine bzw. die für ihn bestimmten Daten selektieren kann.

- Bei Abfragen interner Anwender (Mitarbeiter) erfolgt der Zugriff gesteuert über die Unix/Windows Anmeldung mit eigenem Benutzernamen und Passwort, sowie auf Applikationsebene mit Benutzernamen und zweitem Passwort.
- Ein direkter Zugriff, oder ein unmittelbarer Zugriff auf Datenbankebene ist jedem Anwender verwehrt, und erfolgt ausschließlich über eigene Anwendungsapplikationen.
-

d. Sicherheit des Zugangs zu Applikationen:

- Zugang zu den Applikationen ist nur den dafür freigeschalteten Benutzern möglich. Zugang zu den eigentlichen Anwendungen des Produktionssystems wird zusätzlich noch durch ein zweistufiges Passwort (System/Programme) geschützt, welches nur den betreffenden Entwicklern bekannt ist

e. Zeitliches Sicherheitsmanagement

- Das Authentifizierungs-/Autorisierung-Modul veranlasst nach außen hin bei Nichtaktivität eine automatische Unterbrechung der Verbindung nach 10 Minuten.

4. Gewährleistung, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,

- HOSTPRESS stellt dies durch eine zertifizierte SSL-Verbindung (HTTPS) sicher (s.o.). Sobald diese Verbindung durch eine korrekte Authentifizierung des Benutzers (übereinstimmende ID-Tags wie Benutzererkennung und Passwort, etabliert wurde, ist es nur dem eingeloggten (befugten) Benutzer möglich die Daten zu sehen (nur Leserechte).
- Für alle anderen ist diese verschlüsselte Verbindung nicht „einsehbar". Jeglicher ungeschützter Verbindungsversuch über HTTP führt zu einem Verbindungsabbruch und zur Termination der Session.
- Sämtliche Datenträger der PC- und Notebook Systeme, die zum Zugriff auf das Rechenzentrum der SERVERANBIETER berechtigt sind, sind vollständig verschlüsselt.

5. Weitergabekontrolle

- HOSTPRESS gewährleistet die Weitergabekontrolle, d.h. dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch folgende Maßnahmen:
- Es laufen diverse Protokolle die alle Programmaufrufe dokumentieren (wer sich wann und wie oft eingeloggt hat) und die es ermöglichen zu überprüfen, ob und welche Dateneingaben, Datenbewegungen oder/und ein Datendruck erfolgt sind.
- Jeder Zugriff (wer, wann, wie oft etc.) und jede Veränderung der Datenbank werden durch ein mitgeloggt. Diese Daten werden in Logfiles abgelegt.
- Einrichtungen von Standleitungen bzw. VPN Tunneln zur Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

6. Eingabekontrolle

- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
- HOSTPRESS kann dies feststellen, da grundsätzlich protokolliert wird welche Daten, wann geändert wurden, wie auch systemintern mitgeloggt wird, wer zuletzt welche Daten geändert hat.
- Eingehende Requests und an Clients zurückgesendete Responses des Application-Servers werden in Log-Dateien protokolliert. Die Logdateien werden je nach Last/Frequenz/Platzbedarf einen angemessenen Zeitraum (1 Woche bis 1 Monat) lang aufbewahrt und dann endgültig von einem Applicationserver-Admin gelöscht.

7. Auftragskontrolle

- Die Auftragskontrolle bedeutet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen.
- Dies wird von HOSTPRESS dadurch gewährleistet, dass nur Berechtigte zugreifen können.
- Ausschließlichkeit: Es erhält nur ausdrücklich Berechtigte Zugriff zu den Daten. Durch diese strikte Trennung wird sichergestellt, dass auf die Daten nicht zugegriffen werden kann um sie weiterzuverarbeiten.
- Eine Neuentwicklung oder Programmänderung im Authentifikations- / Autorisierungsmodul erfolgt stets nur bei Vorliegen eines schriftlichen Auftrages, dessen Gültigkeit durch den Geschäftsführer bestätigt werden muss. Diese Aufträge werden ohne zeitliche Beschränkung aufbewahrt. Die Weisungsgebundenheit, Hinweispflichten und Prüfungsrechte sind vertraglich geregelt.
- Weisungen werden grundsätzlich schriftlich erteilt. In Ausnahmefällen können die bevollmächtigten Personen Weisungen auch mündlich erteilen, wobei eine schriftliche Bestätigung erfolgen muss.
- Gewährleistung, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

8. Verfügbarkeitskontrolle / Datensicherung

- Alle Daten werden in einem einheitlich festgelegten Konzept gesichert.
- Die Sicherung erfolgt auf eigens dafür angelegte Sicherungsserver mittels verschlüsselter Übertragung. Zudem werden die zu sichernden Daten vorher lokal ebenfalls verschlüsselt. Sie sind somit nur verschlüsselt auf dem Sicherungsserver gespeichert.
- Am Wochenende findet eine Vollsicherung der Dateisysteme statt. Von Montag bis Freitag werden sie inkrementell gesichert, d.h., nur die Änderungen im Datenbestand werden gesichert.
- Zur Rekonstruktion von Daten liegen sehr ausführliche Anweisungen vor. Nur die Systemadministration ist befugt, aus den Sicherungen zerstörte Dateiinhalte zurückzuholen. Die Rekonstruktion kann nur in den Administrationskennungen ausgeführt werden. In dieser Kennung wird die Recovery-Funktion der Sicherungssoftware benutzt, in der auch die richtigen Datenträger benannt werden.
- Der Systemadministrator führt solche Arbeiten in Eigenverantwortung aus, sein Vertreter auf ausdrückliche Anweisung.
-

9. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden

- Die verschiedenen Datenbereiche sind logisch voneinander getrennt.
- Die Benutzerverwaltung (Stammdaten) ist von der Produktionsdatenverwaltung getrennt. Die Daten der HostPress-Dienste in den Rechenzentren der SERVERANBIETER werden gesondert auf anderen Servern als die Stammdaten gespeichert.
- In der jeweiligen Auftrags-Verwaltung können nur die zugehörigen Kunden eingesehen und verwaltet werden. Dies wird durch festgelegte Benutzerrechte sichergestellt.
- Zum anderen werden separat von der Benutzerverwaltung in der Prozessdatenverwaltung die Login-Daten und die Protokollierungen festgehalten. Es findet keine Weitergabe an Dritte oder sonstige Datenverarbeitung statt. HOSTPRESS speichert die Daten nur und verwendet Sie nur zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Auftraggeber.

II. Technische und organisatorische Maßnahmen der Gridscale GmbH

Anhang „Technisch-organisatorische Maßnahmen"

Nach § 9 BDSG bzw. Art. 32 DSGVO

§ 1. Technische und organisatorische Sicherheitsmaßnahmen
Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG bzw. Art. 32 DSGVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

In anderen Worten,

sind wir als Cloud- und Hostingprovider dazu verpflichtet, ein Höchstmaß an Sicherheit für den Schutz von sensiblen, insbesondere personenbezogenen Daten zu gewährleisten.

§ 2. Innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

In anderen Worten,

wir werden zu jeder Zeit jede Maßnahme ergreifen, die den Schutz vertraulicher, persönlicher und personenbezogener Daten gewährleistet.

§ 3. Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt:

§ Vertraulichkeit (Art. 32 Abs. 1 lit. b. DSGVO)
• Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die Sicherung von Räumlichkeiten erfolgt durch Zutrittsregelung (nur einzelnen Personen wird nach vorheriger Anmeldung Zutritt gewährt), persönliche RFID-Karten zzgl. eines persönlichen biometrischen Merkmals (Fingerabdrucks), elektrische Türöffner, Vereinzelungsanlagen, einen 24/7 Werkschutz, Alarmanlagen und Videoanlagen an allen Ein- und Ausgängen sowie in den Räumlichkeiten selbst;
• Zugangskontrolle
Keine unbefugte Systembenutzung. Jeder Benutzer hat persönliche Zugangsdaten. Es kommen ausschließlich sichere Kennwörter zum Einsatz. Zugänge werden automatisch gesperrt, wenn ein Verdacht auf Manipulation vorliegt. Eine Zwei-Faktor-Authentifizierung ist obligatorisch und sämtliche Datenträger werden verschlüsselt;
• Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems. Dazu kommen Berechtigungskonzepte zum Einsatz. Zugriffsrechte werden nach dem Deny-Allow-Prinzip erteilt und auf das nötigste beschränkt. Jeder Zugriff wird Protokolliert;
• Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B.: Mandantenfähigkeit, Sandboxing, Trennung von Test- und Produktumgebungen;
• Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten findet in einer Weise statt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

In anderen Worten,

um die Vertraulichkeit zu sichern, schützen wir alle unsere Server und Datenspeicher vor unbefugtem, physischen Zugriff mit allen verfügbaren Mitteln. Die Nutzung unserer Systeme oder Services ist ohne persönliche Zugangsdaten ausgeschlossen. Niemand – auch nicht unsere Mitarbeiter – haben unmittelbaren Zugriff auf deine Daten. Grundsätzlich vergeben wir nur solche Benutzerrechte (ggf. temporäre Rechte), die unbedingt für die Arbeit unserer Mitarbeiter erforderlich sind und protokollieren jeden Vorgang.
Informationen, die wir zum Beispiel für unsere Entwicklungsprozesse benötigen, beinhalten niemals persönliche Daten. Wir gewährleisten, dass ein Datenexport vertraulicher Daten niemals möglich ist. Sollten wir doch irgendwann einmal personenbezogene Daten verarbeiten, werden wir diese Daten durch algorithmische Maßnahmen so anonymisieren, dass aus den Daten keine natürliche Person erkennbar ist.

§ Integrität (Art. 32 Abs. 1 lit. b DSGVO)
• Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport. Dazu wird nach aktuellen wissenschaftlichen Erkenntnissen auf Verschlüsselung der Daten sowie Datenübertragung durch Virtual Private Networks (VPN) gesetzt. Daten werden vor Übertragung mit Prüfsumme versehen, um die Unveränderte Übertragung validieren zu können;
• Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu werden Änderungen und Eingaben von Daten protokolliert. Dokumente werden in einem Dokumentenmanagementsystem verwaltet.

In anderen Worten,

die Datenintegrität stellen wir sicher, indem wir stets mit starker Verschlüsselung arbeiten und eine ungewollte Veränderung von Daten über die Anwendung von Prüfsummen umgehend identifizieren.

Das Erstellen neuer oder Ändern bestehender Daten protokollieren wir für die bessere Nachvollziehbarkeit. Wir können also erkennen, „wer" „wann" „was" gemacht hat.

§ Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
• Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch eine online Backup-Strategie (off-site), eine unterbrechungsfreie Stromversorgung (USV), redundanter Hardware, Netztrennungen und dem Einsatz von Firewalls sowie der Gewährleistung einer schnellen Wiederherstellung von Services im Fehlerfall.
• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

In anderen Worten,

wir überwachen alle unsere Dienste und tun alles in unserer Macht stehende für die höchstmögliche Verfügbarkeit und höchstmögliche Sicherheit. Wir sichern zwar unsere eigenen Daten, nicht aber deine Daten.
Wir üben regelmäßig verschiedene Ereignisse, um uns auf eine große Störung vorzubereiten und um dann sofort zu wissen, was wir tun müssen.

§ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
• Datenschutz-Management;
• Incident-Response-Management;
• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
• Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers. Dazu liegt eine eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement vor und etwaige Dienstleisters werden nach strengen Kriterien ausgewählt. Es finden angemessene Kontrollen und Nachkontrollen statt.

In anderen Worten,

wir stellen jederzeit einen sehr guten Datenschutz sicher und sorgen für einen datenschutzfreundlichen Betrieb. Niemals führen wir ohne deinen Auftrag eine Verarbeitung deiner vertraulichen oder persönlichen Daten durch. Außerdem gewährleisten wir, dass 24/7 erfahrene Ingenieure den Betrieb sicherstellen.

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO:
Technische und organisatorische
Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- **Zutrittskonstrolle**
  - **Datacenter-Parks in Nürnberg und Falkenstein**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
  - **Verwaltung**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
  - für Managed Server, Webhosting und Nextcloud
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner,
Stephan Konvickova, Günther Müller
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25
91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- **Zugriffskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Nextcloud
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- **Datenträgerkontrolle**
  - **Datacenter-Parks in Nürnberg und Falkenstein**
    - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).
- **Trennungskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Trennungskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Nextcloud
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner,
Stephan Konvickova, Günther Müller
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25
91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

- **Pseudonymisierung**
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

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

- **Weitergabekontrolle**
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- **Eingabekontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Nextcloud
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

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

- **Verfügbarkeitskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
    - Monitoring aller relevanten Server.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Datensicherung obliegt dem Auftraggeber.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner,
Stephan Konvickova, Günther Müller
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25
91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - für Managed Server, Webhosting und Nextcloud
        - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
        - Einsatz von Festplattenspiegelung.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Einsatz von Softwarefirewall und Portreglementierungen.
        - Dauerhaft aktiver DDoS-Schutz.
- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
    - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**
    - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
    - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
    - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner,
Stephan Konvickova, Günther Müller
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25
91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

IV. Technische und organisatorische Maßnahmen der Krämer IT Solutions GmbH

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO
Verantwortliche Stelle: Krämer IT Solutions GmbH, Koßmannstr. 7 66571 Eppelborn

Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, zu beurteilen, ob die getroffenen Datensicherheits-maßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages.

Standortdefinitionen:

- Standort Eppelborn, Koßmannstrasse7, 66571 Eppelborn
  Nachfolgend als „Zentrale“ bezeichnet

- Standort Losheim, Prof.-Pirlet-Straße 27 – 29, 66679 Losheim am See, Rechenzentrum KÜS
  Nachfolgend als „RZ-KÜS“ bezeichnet

- Standort Saarwellingen, 66793 Saarwellingen, Rechenzentrum VSE
  Nachfolgend als „RZ-VSE“ bezeichnet

- Standort Saarbrücken, Am Felsbrunnen 15, 66119 Saarbrücken
  Nachfolgend als „RZ-SB“ bezeichnet

- Standort Wiesbach, Hauptstraße 1, 66571 Eppelborn
  Nachfolgend als „Landheim“ bezeichnet

1. Pseudonymisierung
Zentrale: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-KÜS: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-VSE: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-SB: Keine Maßnahmen zur Pseudonymisierung von Daten
Landheim: Keine Maßnahmen zur Pseudonymisierung von Daten

2. Verschlüsselung

Zentrale:
- Verschlüsselung von Datentransfers für externe Zugriffe der Mitarbeiter mit VPN
- Verschlüsselter Zugang zum e-mail-Server mit SSL
- Verschlüsselter Fernwartungszugang zu Kunden über VPN
- Verschlüsselung des Mailverkehrs mit ausgewählten Empfängern
  Verschlüsselung von sensiblen e-mail-Anhängen an alle Empfänger

RZ-KÜS:
- Verschlüsselter Datentransfer zwischen RZ-KÜS und anderen Standorten mit VPN

RZ-VSE:
- Verschlüsselter Zugang zum ERP-System mit SSL
- Verschlüsselter Datentransfer zwischen RZ-VSE und anderen Standorten mit VPN
- Verschlüsselte Datenablage mit Zugriff über SSL (Saar-Storage)

RZ-SB:
- Verschlüsselter Datentransfer zwischen RZ-SB und anderen Standorten mit VPN

Landheim:
- Verschlüsselung von Datentransfers für externe Zugriffe der Mitarbeiter mit VPN

3. Vertraulichkeit

Zentrale:
- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Sensible Bereiche wie z.B. Serverraum sind zusätzlich durch Fenstergitter abgesichert
- Zugang zum Serverraum nur für autorisierte Personen (elektronische Zugangskontrolle)
- Alarmanlage
- Individueller Login für alle Mitarbeiter beim Anmelden ans Unternehmensnetzwerk
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Kennwörter müssen regelmäßig geändert werden (180 Tage)
- Kennwortchronik wird erzwungen für 24 gespeicherte Kennwörter
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

RZ-VSE:
- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

RZ-KÜS:
- 24/7 Pförtner, Zugang mit Ausweiskarte mit Bild
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

RZ-SB:
- Begleiteter Zugang nach Anmeldung für autorisierte Mitarbeiter
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

Landheim:
- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Individueller Login für alle Mitarbeiter beim Anmelden ans Unternehmensnetzwerk
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Kennwörter müssen regelmäßig geändert werden (180 Tage)
- Kennwortchronik wird erzwungen für 24 gespeicherte Kennwörter
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

4. Integrität

Alle Standorte:

- Erteilung von Weisungen in schriftlicher Form (Ticket-System)
- Festgelegte Personen bzgl. Empfang und Erteilung von Anweisungen
- Automatisierte Prüfung der relevanten Dateisysteme auf Fehler (Monitoring)
- Regelmäßige zentral gesteuerte und überwachte Updates der Betriebssysteme
- Regelmäßige zentral gesteuerte und überwachte Updates der genutzten Programme
- Zentral gesteuerter und überwachter Viren- Malware- und Ransomware-Schutz

RZ-VSE:
- Systemseitige Protokollierung von Eingaben im ERP-System

5. Verfügbarkeit

Zentrale:
- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Datensicherung auf direkt verfügbare Systeme zur schnellen Datenwiederherstellung im Verlustfall (Backup-to-Disk)
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Brandmeldeanlage
- Temperaturüberwachung sensibler Bereiche
- Feuchtigkeitssensoren, Wassereinbruchsmelder
- Unterbrechungsfreie Stromversorgung für alle Systeme mit Datenhaltung
- Separater Stromkreis

RZ-KÜS:
- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Zertifizierung nach DIN EN 50600 (Teil1 und 2)
- Löschanlage mit einem System zur Brandfrüherkennung
- Klimatisierung
- Redundante Stromversorgung
- 24/7 Objektüberwachung durch einen Sicherheitsdienst
- 24/7 Videoüberwachung des kompletten Geländes und der Gebäude

RZ-VSE:

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Redundante 10 kV Stromzuführung
- Redundante Notstromversorgung
- TIER 4 Elektrotechnikstandards
- Löschgasanlage
- Schaltbare PDUs
- Klimatisierung
- Redundante Stromversorgung

RZ-SB:

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Klimatisierung
- Zertifizierung nach ISO/IEC 27001
- Videoüberwachung und Aufzeichnung im Gebäude und auf der Außenanlage
- Monitoring der kompletten Infrastruktur
- redundante Anbindung an Internet-Backbones
- unterbrechungsfreie Stromversorgung mit redundanter Gebäudezuführung
- Leckage Warnanlage zum Schutz vor Wassereinbrüchen

Landheim:

- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

6. Belastbarkeit der Systeme

Zentrale:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Zentral verwaltete Anti-Ransom-Lösung
- Unterbrechungsfreie Stromversorgung für alle Systeme mit Datenhaltung
- Separater Stromkreis für Serverraum
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung bei Bedarf
- Monitoring aller relevanten Ressourcen
- Einsatz von RAID-Systemen
- Redundante Virtualisierungshost-Systeme

RZ-KÜS:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

RZ-VSE:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

RZ-SB:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

Landheim:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Zentrale:
- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-VSE:
- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-SB:
- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-KÜS:
- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

Landheim:
- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Alle Standorte:
- Regelmäßige Überprüfung der TOMs durch Serientermine sichergestellt
- Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen durch entsprechende Tasks und Checklisten im ERP-System