

Auftragsverarbeitungs-Vertrag (AV-Vertrag)

gemäß Art. 28 Abs. 3 der EU-Datenschutz-Grundverordnung (EU-DSGVO)

zwischen

Herrn
Richard Scheglmann
Theodor-Heuss-Straße 9
85764 Oberschleißheim
Deutschland
(Kunden-Nummer 17396)

- *nachstehend „Auftraggeber“ genannt* -

und

manitu GmbH
Welvertstraße 2
66606 St. Wendel
Deutschland

- *nachstehend „Auftragnehmer“ genannt* -

zu

allen (aktuellen und künftigen) Verträgen zwischen dem Auftraggeber und dem Auftragnehmer unter der o.g. Kunden-Nummer

- *nachfolgend „Hauptvertrag“ genannt* -

Präambel

Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Hauptvertrag ergeben.

Dieser Vertrag findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen, und bei denen Beschäftigte / Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

§ 1 Gegenstand der Auftragsverarbeitung

1. Aus dem Hauptvertrag (basierend auf den AGB, den Leistungsbeschreibungen, der Webseite sowie den Angeboten und Auftragsbestätigungen des Auftragnehmers) ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Konkret umfasst dies die Bereitstellung von Hosting-Dienstleistungen (Webhosting, Root-Server etc.). Im Rahmen dieser Hosting-Dienstleistungen hat der Auftraggeber die Möglichkeit, selbständig mit Daten auf Systemen des Auftragnehmers umzugehen (speichern, verändern, löschen, übertragen, verarbeiten, berichtigen etc.).

2. Explizit **nicht** Gegenstand dieses Vertrages und explizit **nicht** des Hauptvertrages ist eine originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragnehmer. Die Regelungen dieses Vertrages sind nötig, da nicht ausgeschlossen werden kann, dass der Auftragnehmer im Zuge der Leistungserbringung des Hauptvertrages mit Daten des Auftraggebers in Berührung kommen kann.

3. Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages und endet automatisch, wenn der Hauptvertrag endet, sofern sich aus gesetzlichen Bestimmungen nicht darüber hinausgehende Verpflichtungen ergeben. Darüber hinaus kann dieser Vertrag von jeder Vertragspartei mit einer Frist von 1 Monat ordentlich gekündigt werden. Das Recht zur

außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Eine Kündigung dieses Vertrages beinhaltet keine Kündigung des Hauptvertrages und bedingt diese auch nicht.

§ 2 Pflichten des Auftraggebers

1. Der Auftraggeber ist alleine für die Einhaltung der datenschutzrechtlichen Bestimmungen und Gesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, für die Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (*Verantwortlicher* im Sinne des Art. 4 Nr. 7 EU-DSGVO).
2. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollumfänglich zu informieren, wenn er Verstöße des Auftragnehmers gegen datenschutzrechtliche Bestimmungen oder Gesetze feststellt.
3. Der Auftraggeber ist alleine gegenüber betroffenen Personen verantwortlich, mit dessen Daten er auf Systemen der Auftragnehmers umgeht, insbesondere was das Recht auf Auskunft, Berichtigung, Löschung oder Sperrung angeht. Er ist alleine für die Wahrung der Rechte der betroffenen Personen verantwortlich.
4. Der Auftraggeber ist alleine für alle Informationspflichten, insbesondere gegenüber betroffenen Personen, verantwortlich.
5. Der Auftraggeber ist verpflichtet, alle im Rahmen dieses Vertrages erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers u.ä. - auch über die Beendigung des Vertrages hinaus - vertraulich zu behandeln und in keinem Fall an Dritte weiterzugeben. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch den Auftragnehmer als vertraulich zu behandeln. Der Auftraggeber ist berechtigt, Dokumentationen für den Nachweis der Erfüllung seiner Sorgfaltspflichten und seiner gesetzlichen Verpflichtungen zu erstellen, soweit Geschäftsinteressen, Geheimhaltungsinteressen oder Sicherheitsinteressen des Auftragnehmers

dem nicht entgegenstehen. Für etwaige Schäden sowie Folgeschäden aus der Verletzung der vorgenannten Geheimhaltungspflicht des Auftraggebers haftet dieser gegenüber dem Auftragnehmer zeitlich und finanziell unbegrenzt.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf die ihm vom Auftraggeber zur Verfügung gestellten personenbezogenen Daten von betroffenen Personen nur im Rahmen des Hauptvertrages und zur Erfüllung der darin beinhalteten Leistungen verwenden. Eine Verwendung für Zwecke außerhalb des Hauptvertrages findet nicht statt. Kopien oder Duplikate werden nur erstellt, wenn dies dem Charakter des Hauptvertrages und den darin beinhalteten Leistungen entspricht (z.B. Datensicherungen, temporäre Dateien, Log-Dateien etc.).

2. Sofern eine gesetzliche Verpflichtung besteht, ist der Auftragnehmer zur Herstellung von Kopien oder zur Weitergabe von Daten des Auftraggebers ermächtigt. Eine Information erfolgt im Rahmen der gesetzlichen Bestimmungen.

3. Die Datenverarbeitung durch den Auftragnehmer erfolgt ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, sofern nichts Anderes vom Auftraggeber beauftragt wurde, und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

4. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird dazu angemessene technische und organisatorische Maßnahmen (TOM) zum angemessenen Schutz der Daten des Auftraggebers treffen und aufrechterhalten, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 EU-DSGVO) genügen, insbesondere in Bezug auf die Vertraulichkeit und Integrität. Diese technischen und organisatorischen Maßnahmen sind diesem Vertrag als Anlage beigefügt. Beide Vertragsparteien verständigen sich darauf, diese

technischen und organisatorischen Maßnahmen als ausreichenden Nachweis für die Verpflichtungen, die sich aus diesem Vertrag ergeben, zu sehen. Die technischen und organisatorischen Maßnahmen sind dem Auftraggeber dadurch bekannt und er trägt die alleinige Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. 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 sorgt dafür, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb dieses Vertrages und des Hauptvertrages zu verarbeiten. Ferner sorgt der Auftragnehmer dafür, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtung besteht auch nach Beendigung dieses Vertrages und des Hauptvertrages fort, sofern dies aus dem Charakter des Hauptvertrages hervorgeht.

6. Der Auftragnehmer unterrichtet den Auftraggeber, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers, welche durch den Auftragnehmer verursacht wurden, bekannt werden.

7. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahmung oder durch ein Insolvenz- oder Vergleichsverfahren gefährdet werden, so hat der Auftragnehmer den Auftraggeber darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der EU-DSGVO liegen.

8. Der Auftragnehmer ist gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer dient der jeweils auf der Webseite des

Auftragnehmers angegebene, freiwillig bestellte, interne Datenschutzbeauftragte.

§ 4 Anfragen betroffener Personen

1. Wendet sich eine betroffene Person an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern dies nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer wird derartige Anfragen nicht bearbeiten, nicht beantworten und insbesondere keine Änderungen etc. an Daten vornehmen oder Auskünfte erteilen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

2. Der Auftragnehmer unterstützt, soweit vereinbart und zumutbar und soweit dies dem Charakter des Hauptvertrages und den darin beinhalteten Leistungen entspricht, den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im Rahmen seiner technischen und betrieblichen Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gemäß Kapitel III der EU-DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 EU-DSGVO genannten Pflichten.

§ 5 Umgang mit Daten

1. Der Auftraggeber hat im Rahmen der Leistungen des Hauptvertrages jederzeit selbst und vollumfänglich Zugriff auf seine Daten, so dass eine Mitwirkung des Auftragnehmers zum Umgang mit Daten nicht nötig ist und daher nicht stattfindet.

2. Erteilt der Auftraggeber dem Auftragnehmer Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang des Hauptvertrages hinausgehen, müssen diese schriftlich erfolgen. Die die dadurch begründeten Kosten/Aufwendungen sind vom Auftraggeber zu tragen. Die Durchführung solcher Einzelanweisungen erfolgt nur nach vorheriger Bestätigung durch den

Auftragnehmer. Der Auftragnehmer kann und darf solche Einzelanweisungen – auch generell – ablehnen oder aussetzen, insbesondere wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt.

3. Da es im Rahmen des Hauptvertrages nicht zu einem Datenträgeraustausch kommt, entfällt die Notwendigkeit zur Regelung einer Rückgabe oder Löschung. Für die Löschung von Daten nach Ende des Hauptvertrages ist der Auftraggeber gemäß Absatz 1 und gemäß dem Charakter des Hauptvertrages und der darin beinhalteten Leistungen in der Lage und alleine verantwortlich. Evtl. entstandene Datensicherungen etc. gemäß dem Charakter der im Hauptvertrag beinhalteten Leistungen werden gemäß der technischen und organisatorischen Maßnahmen innerhalb angemessener Frist durch den Auftragnehmer gelöscht.

§ 6 Art der personenbezogenen Daten, betroffene Personen

1. Die Daten, mit denen der Auftraggeber umgeht, können nach Art. 4 Nr. 1, 13, 14 und 15 DSGVO mehrere oder alle Arten von Daten wie nachfolgend beschrieben oder darüber hinaus enthalten: Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorien, Vertrags- und Zahlungsdaten, Auskunftsangaben, Bestell- und Angebotsdaten, Bild- und Videodaten, Personaldaten, Transaktionsdaten, Bank- oder Kreditkartendaten, sonstige Daten etc.

2. Der Kreis der betroffenen Personen der Daten, mit denen der Auftraggeber umgeht, kann nach Art. 4 Nr. 1 EU-DSGVO mehrere oder alle oder darüber hinaus gehende Kreise wie nachfolgend beschrieben, umfassen: Kunden, Interessenten, Abonnenten, Mitglieder, Beschäftigte/Mitarbeiter, Lieferanten, Dienstleister, Vermittler, Geschäftspartner, sonstige betroffene Personen etc.

§ 7 Kontrollen

1. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten

Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens jedoch 6 Wochen) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit der angegebenen Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung, von betrieblichen Bedürfnissen und den technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Während der Prüfung wird für jede anwesende Person im Auftrag des Auftraggebers ein Mitarbeiter des Auftragnehmers anwesend sein. Als Vergütungsbasis für den Aufwand, der dem Auftragnehmer durch eine Inspektion entsteht, verständigen sich beide Vertragsparteien auf eine Abrechnung in ganzen Arbeitstagen zu jeweils 10 Arbeitsstunden je anwesendem Mitarbeiter des Auftragnehmers.

2. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 1, auch in Bezug auf die Regelungen zum Aufwand, 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.

§ 8 Subunternehmen (Untervertragsverhältnisse)

1. Der Auftragnehmer darf weitere Auftragsverarbeiter nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

2. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Der Auftragnehmer wird dazu mit diesen Subunternehmern in erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

3. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse / weiteren Auftragsverarbeiter dar. Nebenleistungen in diesem Sinne sind insbesondere aber nicht ausschließlich Reinigung, Wartung, Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, und die keinen konkreten Bezug zur Hauptleistung aufweisen.

§ 9 Haftung, Schadensersatz, Vertragsstrafe

1. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber oder gegenüber betroffenen Personen für Schäden, die sich aus Verletzungen seiner Pflichten aus diesem Vertrag ergeben, werden vollumfänglich ausgeschlossen.

2. Der Auftraggeber stellt den Auftragnehmer dauerhaft, auch über das Ende dieses Vertrages hinaus, von allen Ansprüchen, die sich u.a. aus Art. 82 EU-DSGVO ergeben frei - auch in Fällen, in denen der Schaden durch eine Verletzung der Pflichten durch Fahrlässigkeit oder grobe Fahrlässigkeit durch den Auftragnehmer entstanden ist.

3. Eine Vertragsstrafe wird nicht vereinbart und ausgeschlossen.

4. Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach der EU-DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber der betroffenen Person alleine verantwortlich.

§ 10 Kostenregelung

1. Der Auftraggeber ersetzt dem Auftragnehmer alle mit diesem Vertrag direkt oder indirekt in

Zusammenhang stehenden Aufwände und Kosten, auch solchen, die sich aus gesetzlichen Verpflichtungen oder aus diesem Vertrag ergeben, abgerechnet in ganzen Stunden. Ausgenommen hiervon sind Inspektionen, welche gemäß § 7 abgerechnet werden.

2. Es gelten die regulären Stundensätze des Auftragnehmers.

§ 11 Abschließendes

1. Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile bedürfen einer schriftlichen Vereinbarung. Dies gilt auch für den Verzicht auf diese Formerfordernis.

2. Soweit rechtlich zulässig, wird als Gerichtsstand St. Wendel vereinbart. Es gilt ausschließlich deutsches Recht.

3. Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages den Regelungen des Hauptvertrages vor.

4. Es gelten die Regelungen der Allgemeinen Geschäftsbedingungen (AGB) sowie die Leistungsbeschreibungen des Auftragnehmers.

§ 12 Salvatorische Klausel

1. Sollte eine Bestimmung des Vertrages ungültig oder unwirksam sein oder werden oder sollte der Vertrag unvollständig oder undurchsetzbar sein, so wird der Vertrag in seinem übrigen Inhalt davon nicht berührt. Die unwirksame Bestimmung gilt durch eine solche Bestimmung ersetzt, die dem Sinn und Zweck der unwirksamen Bestimmung in rechtswirksamer Weise wirtschaftlich am nächsten kommt. Gleiches gilt für etwaige Vertragslücken.

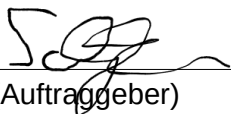
Name: Richard Scheglmann

Name: Manuel Schmitt

Position: Webseitenbetreiber


Position: Geschäftsführer

2020-10-11 23:36:43



Datum, Unterschrift (Auftraggeber)

2020-10-11 23:36:43



Datum, Unterschrift (Auftragnehmer)

Anlage: Technische und organisatorische Maßnahmen (TOM)

Anlage **Technische und organisatorische Maßnahmen (TOM)**

gemäß Art. 32 Abs. 1 EU-DSGVO

1. Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Alarmanlage mit Bewegungs- und Einbruchmeldern sowie Anschluss an Wachdienst
- Videoüberwachung der Zugänge
- Elektronisches Zugangskontrollsystem mit Schließsystem und Sicherheitsschlössern
- Restriktive Schlüsselregelung
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal ¹
- Sorgfältige Auswahl von Sicherheits-/Wachpersonal ¹
- Protokollierung von Besuchern ¹

¹ Besucher und fremde Dienstleister dürfen sich nur in Begleitung von Personal in den relevanten Räumlichkeiten aufhalten.

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Authentifikation für Mitarbeiter nur mit Benutzername + Passwort
- Strenge Passwortregeln für Mitarbeiter
- Umfassende Protokollierung
- Einsatz von Anti-Viren-Software

- Einsatz von Firewalls und IDS
- Einsatz von Verschlüsselung und VPN-Technologien
- Getrennte Netzbereiche für Administrations- und Wartungszwecke

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Restriktive Berechtigungsregelungen
- Umfassende Protokollierung
- Einsatz von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Sichere Löschung von Datenträgern vor Wiederverwendung

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Firmen-Daten von Kunden-Daten strikt getrennt
- Trennung von Produktiv- und Testsystemen

1.5 Pseudonymisierung

Maßnahmen, die sicherstellen, dass Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr oder schwer einer spezifischen betroffenen Person zugeordnet werden können.

- Kurze Vorhaltezeiten von Log-Dateien
- Reduktion von Log-Dateien auf das Nötigste

2. Integrität

1.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Berechtigungssystem zur sowie Protokollierung der Eingabe, Änderung und Löschung von Daten

2.2 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einsatz von Verschlüsselung und VPN-Technologien
- Authentifizierung

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromdiesel-Aggregat
- Feuer- und Rauchmeldeanlage mit Anschluss an Wachdienst
- Feuerlöschgeräte in Serverräumen
- Geräte zur Überwachung von Temperatur in Serverräumen

- Klimaanlage in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backup- und Recovery-Strategie
- Notfallpläne
- Serverräume über der Wassergrenze
- Automatische Überwachungssysteme (Monitoring) kritischer Systeme
- Incident Management

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Verpflichtung der Mitarbeitern und Subunternehmern auf die EU-DSGVO
- Maßnahmen gemäß § 1, 2 und 3 der TOM sowie des AV-Vertrages
- Verarbeitung ausschließlich in der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum

4.2 Datenschutz-Management

Maßnahmen, die gewährleisten, dass der Datenschutz fortlaufend sichergestellt ist.

- Implementierung eines Datenschutz-Managements

4.3 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass der Datenschutz oberste Priorität in allen Belangen hat.

- Reduktion der Pflichtfelder in Formularen auf das Nötigste