Vertrag über die Verarbeitung von Daten im Auftrag nach Art. 28 Abs. 3 DSGVO

Auftraggeber

Mein Paul UG (haftungsbeschränkt), Hirschdorfer Straße 27a, 87493 Lauben
Vertreten durch: Peter Kusel, Herbert Birkenmaier

Auftragnehmer (Kunde)

Präambel

Diese Anlage konkretisiert die Verpflichtung der Vertragsparteien zum Datenschutz, die sich aus den im oben genannten Vertrag – in ihren Einzelheiten beschriebenen Auftragsverarbeitungen 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 im Sinne des Art. 4 Nr. 1 DSGVO) des Auftraggebers verarbeiten.

§ 1 Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

Nutzung der Plattform und/oder der Dienstleistung, MEIN PAUL als:

- **Client Version (Installer)**
- **Webversion**
- **APP**

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages. Der Gegenstand des Auftrags ergibt sich aus der oben genannten Leistungsvereinbarung(en), auf die hiermit verwiesen wird. Der Auftragnehmer erhebt/verarbeitet/nutzt dabei personenbezogene Daten im Auftrag des Auftraggebers oder kann bei der Durchführung des Auftrages mit personenbezogenen Daten in Berührung kommen.

Der Vertrag wird auf unbestimmte Zeit geschlossen. Kündigungsfrist beträgt 4 Wochen.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 2 Konkretisierung des Auftragsinhaltes

(1) Zweck der vorgesehenen Verarbeitung von Daten (entsprechend der Definition von Art. Nr. 2 DSGVO)

Die Verarbeitung von Daten dient der Vertragsanbahnung, dem Vertragsabschluss sowie der Vertragserfüllung zu der oben genannten Leistungsvereinbarung, auf die hiermit verwiesen wird.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- Personenstammdaten
- Kommunikationsdaten (z. B. Telefon, Email)
- Vertragsstammdaten (Vertragsbeziehungen, Produktinteresse)
- Kundenhistorie
- Auskunftsangaben

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mandanten
- Sachbearbeiter
- Sekretariat
- Administratoren

§ 3 Technisch – organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Folgenden dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung festgelegt und in Anlage 1 dokumentiert. Diese Maßnahmen werden Grundlage des Auftrags. Soweit eine Prüfung bzw. ein Audit des Auftraggebers einen Anpassungsbedarf ergeben, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. C, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zu Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Anlage 1).

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

§ 4 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen Werden, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gem. Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gem. Art. 38 und 39 DSGVO ausübt
Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Johannes Landerer bestellt.
Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(2) Die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellt Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zu Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technisch und organisatorischen Maßnahmen gem. Art. 28 Abs. 3 S. 2 lit. C, 32 DSGVO

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen

(5) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technisch und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 8 dieses Vertrages

§ 6 Unterauftragsverhältnisse/Subunternehmen

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Der Auftragnehmer darf Subunternehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu:

Firma	Anschrift	Leistung
Steuerkanzlei Birkenmaier & Kusel	Hirschdorfer Str. 27 a, 87493 Lauben	Verwaltung, Abwicklung, …
Team Nifty GmbH	Fischerstraße 19, 87435 Kempten	Entwicklung
Allgäu Solution UG (haftungsbeschränkt)	Schlingener Str. 4, 86842 Türkheim	Frontendkonzeptionierung, Websiteintegration

(4) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(5) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(6) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(7) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) wie folgt zu überprüfen:

(8) Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

(9) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(10) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. ER hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- Die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO
- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen

§ 8 Mitteilung bei Verstößen

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

(2) Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

(3) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen

§ 9 Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigen der Auftraggeber unverzüglich (mind. Textform)

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(6) Anfragen zum Datenschutz können unter datenschutz@mein-paul.com erfolgen

Anlage – Technisch-/organisatorische Maßnahmen

Technisch und organisatorische Maßnahmen nach der EU- Datenschutzgrundverordnung (DSGVO) des Unternehmens Mein PAUL UG

Generelle Beschreibung

- Vorhandensein von internem IT-Sicherheitskonzept und IT-Sicherheitsrichtlinien
- Datenverarbeitung ist in Arbeits- und Prozessbeschreibungen schriftlich geregelt
- Fremdfirmen haben nur einen Zugriff auf Datenverarbeitung, wenn dies durch einen Auftragsdatenverarbeitungsvertrag geregelt ist
- Vertretungsregelung für IT-Verantwortlichen bei Urlaub oder Krankheit
- Schriftliche Bestellung eines Datenschutzbeauftragten
- Verpflichtung aller Mitarbeiter nachweislich auf das Datengeheimnis
- Regelmäßige Kontrolle bzgl. Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen
- Vorhandensein von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO, soweit eine Verpflichtung gem. Art 30 Abs. 5 DSGVO besteht
- Namentliche Nennung der Ansprechpartner (IT-Verantwortlicher und externer Datenschutzbeauftragter) zur Klärung fachlicher, technischer und organisatorischer Fragen
- Rechenzentrum: Telekom – Open Telekom Cloud
- Verschlüsselung der Daten, soweit dies unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen in Anbetracht der Verarbeitungszwecke möglich ist.

In den folgenden Abschnitten sind einige technische und organisatorisch Maßnahmen gem. Art. 32 DSGVO konkret beschrieben.

1. Zugangskontrolle

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugte den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahmen im Einzelnen:

- Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Schlüsseln zu betreten
- Zusätzlich werden außerhalb der Bürozeiten einbruchshemmende Sicherheitstüren verschlossen
- Ausgaben und Rückgabe von Schlüsseln ist geregelt und dokumentiert
- Definierte Zutrittsregelungen und definierte Sicherheitsbereiche. Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern der Mein Paul UG in das Büro begleitet und können sich nicht unkontrolliert im Geschäftsbereich aufhalten
- Die Mein Paul UG verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren
- Der Zutritt zu den Serverräumen ist durch eine separate Schließanlage abgesichert

2. Datenträgerkontrolle

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird.

Maßnahmen im Einzelnen:

- Firewall-Cluster
- Externer Zugriff von Mitarbeitern ist nur via VPN und Authentifizierung möglich
- Trennung Gäste-WLAN vom Firmennetzwerk
- Anti-Viren Software auf allen eingesetzten IT-Anlagen
- Akten unter Verschluss. Zugang nur für berechtigte Personen
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall-Cluster verhindert ungewollte Zugriffe von außen
- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden
- Alle Firmennotebooks und Tablets sind mit Mobile Devicemanagement und Festplattenverschlüsselung ausgestattet. USB-Anschlüsse sind für externe Datenträger standardmäßig deaktiviert. Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich zu speichern (Speicherung möglichst auf zentralen Servern)
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an die Mein Paul UG zurück

3. Speicherkontrolle

Die Speicherkontrolle umfasst Maßnahmen, mit denen unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

Maßnahmen im Einzelnen:

- Zugriffe auf die Server der Mein Paul UG erfolgen durch die Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz geregelt
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen
- Bei Zugriff auf Daten beim Auftraggeber ist durch die von der Mein Paul UG eingesetzte Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation protokolliert werden
- Wenn ein Mitarbeiter ausscheidet, werden ihm alle Zugriffsrechte entzogen
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeber Bereich zu lesen, zu kopieren, zu ändern oder zu entfernen
- Wenn die Mein Paul UG die Daten von einem Auftraggeber nicht mehr benötig, werden die Datenträger gemäß gesetzlichen Bestimmungen vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht
- Siehe im Übrigen Datenträgerkontrolle und Zugriffskontrolle

4. Benutzerkontrolle

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

Maßnahmen im Einzelnen:

- Siehe Datenträgerkontrolle und Zugriffskontrolle

5. Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Maßnahmen im Einzelnen:

- Vorhandensein eines Berechtigungskonzepts
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes, Verschlüsselung
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten
- Verbot der Nutzung von privatem Datenträger
- Zugriff auf Notebooks, PC, Tablet und Server nur mit Username und Passwort möglich
- Passwörter unterliegen definierten Passwortrichtlinien (hohe Anforderungen)
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort
- Automatische Bildschirmsperre mit Passwort-Aktivierung
- Zugangsprotokollierung
- Sperrung nach mehrfach fehlerhaften Anmeldeversuchen
- Löschung gem. Konzept, Schutzklassen und gesicherte Zwischenlagerung defekter Datenträger bis zu datenschutzkonformer Vernichtung
- Vernichtung ausgedruckter Daten durch zugelassene Unternehmen
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDSs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt

6. Übertragungskontrolle

Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Maßnahmen im Einzelnen:

- Regelungen zur Datenübertragung sind vorhanden
- Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert
- Auftraggeber können die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server der Mein Paul UG übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen

7. Eingabekontrolle

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

Maßnahmen im Einzelnen:

- Regelungen zur Dateneingabe sind vorhanden
- Erstellung und Änderung von Daten wird protokolliert

8. Transportkontrolle

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

Maßnahmen im Einzelnen:

- Firewall-Cluster
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung
- Die Datenfernübertragungssysteme der Mein Paul UG sind mit Datenverschlüsselungen versehen und werden auf dem jeweils aktuellen technischen Stand gehalten
- Statistiken mit personenbezogenen Inhalten werden nur im Auftrag an berechtigte Personen übermittelt

9. Wiederherstellbarkeit

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Maßnahmen im Einzelnen:

- Regelmäßige Überprüfung der gesicherten Daten auf Wiederherstellbarkeit
- Zugriffe auf Festplatten mit Datensicherung nur für Berechtigte
- Datenträgerverwaltung, Datensicherung werden gesichert (in separatem Raum, Tresor, etc.)
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten
- Überwachung von Backupzyklen

10. Zuverlässigkeit

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Maßnahmen im Einzelnen:

- Siehe Verfügbarkeitskontrolle

11. Datenintegrität

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Maßnahmen im Einzelnen:

- Siehe Verfügbarkeitskontrolle

12. Auftragskontrolle

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

Maßnahmen im Einzelnen:

- Alle Mitarbeiter der Mein Paul UG sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten
- Alle bereitgestellten Daten verbleiben ausschließlich in der Verfügungsmacht der Mein Paul UG
- Weitergabe personenbezogener Daten erfolgt im Rahmen der datenschutzrechtlichen Bestimmungen
- Dienstleister der Mein Paul UG unterliegen einem laufenden Überprüfungskonzepts
- Alle Mitarbeiter der Mein Paul UG, die mit personenbezogenen Daten aus dem Bereich der Auftraggeber in Kontakt kommen könnten, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen

13. Verfügbarkeitskontrolle

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

Maßnahmen im Einzelnen:

- Tägliche Datensicherung
- Feuerlöscher in ausreichender Anzahl im Gebäude
- Brandschutztüren
- Vorgaben des Brandschutzes werden eingehalten und regelmäßig durch externe Prüfungen zertifiziert
- Rauchverbot in Büro- und Technikräumen
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz
- Back-Up-Verfahren für Server und Arbeitsplatz-PC’s
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt
- Sicherungskopien (siehe Punkt 9 Datenträgerverwaltung)
- Virenschutzprogramme auf allen Computersystemen
- Firewall-Cluster und aktuelle Viren-scanner zur Absicherung sowohl des zentralen Datenbankservers als auch des Mail-Servers. Die Virensignatur des verwendeten Virenscanners werden täglich mehrfach aktualisiert
- E-Mail Anhänge werden auf Infizierung überwacht

14. Trennbarkeit

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen im Einzelnen:

- Es ist nicht vorgesehen, dass die Mein Paul UG erhobene personenbezogene Daten zu anderen Zwecken verarbeitet