Anlage 1 Gegenstand der betroffenen Daten

Zweck der Datenerhebung, -verarbeitung und -nutzung	Kategorien personenbezogener Daten	Kreis der Betroffenen
Entwicklung, Support und Installation von Archivlösungen.	Archivierung IT-Nutzungsdaten Adressdaten Kommunikationsdaten Zahlungsdaten Name	Mitarbeiter Ehem. Mitarbeiter Kunden Lieferanten Interessenten

Die im Hauptvertrag sowie in den Leistungsbeschreibungen festgelegten Verarbeitungen (IT-Systeme und Anwendungen) sind die Grundlage für den Gegenstand der personenbezogenen Daten.

Anlage 2 Technische und organisatorische Maßnahmen

1 Zutrittskontrolle

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

- ☒ Alarmanlage
- ☒ Automatisches Zutrittskontrollsystem
- ☒ Schließsystem mit Codesperre
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Tragepflicht von Besucherausweisen
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner/Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal

2 Zugangskontrolle

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

- ☒ Zuordnung von Benutzerrechten
- ☒ Vorgaben für sichere Passwörter
- ☒ Authentifikation mit Benutzername/Passwort
- ☒ Einsatz von individuellen Benutzernahmen
- ☒ Einsatz von VPN-Technologie (Fernzugriff)
- ☒ Einsatz von Intrusion-Detection-Systemen

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.

- ☒ Berechtigungskonzept
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Verschlüsselung von Datenträgern
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz von Software-Firewall
- ☒ Rechteverwaltung
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☒ Protokollierung der Vernichtung
- ☒ Einsatz von Anti-Viren-Software

4 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.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ E-Mail-Verschlüsselung

5 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.

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

6 Auftragskontrolle

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

- ☒ Auswahl der (Unter-) Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsdatenverarbeitungsvertrag)
- ☒ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/Vertraulichkeit
- ☒ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)

7 Verfügbarkeitskontrolle

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

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleiste in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- und Recoverykonzeptes
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☒ Serverräume nicht unter sanitären Anlagen

8 Trennungsgebot

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

☒ Festlegung von Datenbank-Rechten

☒ Logische Mandantentrennung (softwareseitig)

☒ Trennung von Produktiv- und Testsystem

☒ Keine Produktivität in Testsystemen

Anlage 3 Übersicht der Subunternehmer

Nr.	Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung
1	SEG System-EDV und Organisationsgesellschaft mbH Borsteler Chaussee 49 22453 Hamburg	Support von Archivlösungen	Deutschland

Anlage 4 Empfangsberechtigte Personen

Zum Empfang von Weisungen betreffend die Auftragsdatenverarbeitung sind aufseiten des Auftragnehmers ausschließlich folgende Personen berechtigt:

Name	Position	Telefon	E-Mail
Dennis Skora	Leiter Marketing	05136 898 8008	datenschutz@vaps.de
Andreas Meier	Leiter Applikationen & Services	05136 898 6281	datenschutz@vaps.de
Alexander Salfeld	Informationssicherheitsbeauftragter	05136 898 6234	datenschutz@vaps.de

Beim Auftragnehmer ist folgende Person als Datenschutzbeauftragte/r bestellt:

Thomas Althammer, externer Datenschutzbeauftragter, 05113 306 0390, datenschutz@vaps.de, kontakt-dsb@althammer-kill.de

Anlage 5 Mobiles Arbeiten

Definition

Mobiles Arbeiten beschreibt die arbeitsvertraglich vereinbarte Tätigkeit außerhalb der Betriebsstätte des Arbeitgebers. Sowohl ganztägiges als auch tagesanteiliges mobiles Arbeiten ist möglich. Nach Vereinbarung kann die Arbeit an verschiedenen Arbeitsorten und zu verschiedenen Tageszeiten innerhalb und außerhalb der Betriebsstätte geleistet werden.

Mobiles Arbeiten unterscheidet sich von Homeoffice. Eine gesetzliche Definition des Begriffes Homeoffice gibt es (noch) nicht. Nach dem allgemeinen Sprachgebrauch versteht man hierunter das gelegentliche oder ständige Arbeiten in den privaten Räumlichkeiten des/der Mitarbeiter*in. Unter mobilem Arbeiten versteht man hingegen die unter Zurverfügungstellung von mobilen Endgeräten eingeräumte Möglichkeit, die Arbeitsleistung an typischerweise wechselnden Orten außerhalb des Betriebs zu erbringen (etwa auf Reisen im Zug, im Hotel oder auf dem heimischen Sofa). Die Mitarbeiter*innen müssen nicht notwendig von zuhause arbeiten.

Schutz von Informationen & Datenschutz

Jeder Benutzer hat sicherzustellen, dass jederzeit ein zu den Geschäftsräumen vergleichbares Sicherheitsniveau („Clean Desk“, Schutz vor Mithören und Einsichtnahme) vorhanden ist. Insbesondere müssen Informationen vor unberechtigten Dritten (Familienmitglieder, Mitbewohner) entsprechend ihrer Klassifizierung geschützt werden.

Ebenfalls muss vom Benutzer die verwendete Infrastruktur (z.B. Router/Internetverbindung) nach dem Stand der Technik abgesichert sein. Der Zugang zum Netzwerk der Organisation hat über eine von der Organisation bereitgestellte VPN-Verbindung zu erfolgen.

Die auf die jeweiligen Arbeitsverhältnisse anzuwendenden datenschutzrechtlichen Hinweise gelten gleichermaßen für das mobile Arbeiten.

Es wird ausdrücklich darauf hingewiesen, dass es den Mitarbeitenden untersagt ist, dienstliche Unterlagen mitzunehmen und außerhalb der Diensträume aufzubewahren.

Bei der Entsorgung von Dokumenten ist sicherzustellen, dass diese ordnungsgemäß vernichtet werden. Ist dies nicht möglich, so sind die Dokumente ordnungsgemäß in den Geschäftsräumen des Unternehmens zu entsorgen.

Mobile IT-Systeme müssen an einem sicheren Ort aufbewahrt werden, wenn sie längere Zeit unbeobachtet sind.