Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

vacos.time

Im Folgenden sind die technischen und organisatorischen Maßnahmen zu dokumentieren, die vom Auftragsverarbeiter für die Gewährleistung der Sicherheit der Datenverarbeitung umgesetzt werden. Nicht alle im Folgenden aufgelisteten Maßnahmen sind umzusetzen, es ist jeweils ein in der Gesamtheit dem Risiko der Verarbeitung angemessener Schutz entsprechend dem Stand der Technik durch den Auftragsverarbeiter zu gewährleisten. Beim Stand der Technik handelt es sich um bewährte und effektive Maßnahmen, die derzeit auf dem Markt verfügbar sind.

1.1 Vertraulichkeit der Systeme und Dienste

1.1.1 Physischer Schutz (Zutrittskontrolle)

- Festlegung und Dokumentation zutrittsberechtigter Personen, einschließlich des Umfanges der Berechtigung
- Gelebte Regelung für den Zutritt von Firmenfremden (z.B. Begleitung, Zutrittsverbote, Ausweise)
- Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung
- Einbruchhemmende Fenster im Erdgeschoss/Keller
- Arbeitsplatzrechner sind in verschlossenen Räumen
- Ausdruck-Erstellung an definierte Gebäude-Zonen gebunden oder durch persönliches Drucken (z.B. Print-to-me, follow-me print, mit PIN)
- Aktenvernichtung ausschließlich innerhalb definierter Zonen (z.B. durch Schredder)

1.1.2 Schutz des Systemzugangs (Zugangskontrolle)

- Passwörter werden nicht im Klartext gespeichert
- Passwörter werden nach dem Stand der Technik gehashed gespeichert
- Veröffentlichung von Passwortregeln für Mitarbeiter (z.B. Verbot der Weitergabe, der Speicherung im Browser oder der Mehrfachverwendung)
- Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer (z.B. verschlüsselte Mail, getrennte Briefe für Benutzername und Passwort)
- Berechtigungskonzept für IT-Applikationen/IT-Systeme
- Weitere Interaktionen mit dem IT-System sind nur nach einer erfolgreichen Authentifizierung möglich
- Einsatz von Zwei- oder Mehr-Faktor-Authentifizierung bei Systemzugängen zu kritischen Inhalten und Admin-Konten

1.1.3 Berechtigungsmanagement (Zugriffskontrolle)

- Es werden nur eindeutige und personalisierte Benutzerkonten verwendet
- Zugriffsberechtigungen nur gemäß Erforderlichkeitsprinzip („Need-to-Know“) und mit den geringsten möglichen Rechten („Least Privilege“)
- Regelmäßige Überprüfung (z.B. einmal pro Jahr) der Berechtigungen
- Veränderungen der Zuständigkeiten/Arbeitsverhältnisse von Mitarbeitern führen zu umgehender Anpassung der Zugänge und Rechte

1.1.4 Verschlüsselung und Pseudonymisierung

- Die elektronische Übermittlung von personenbezogenen Daten erfolgt verschlüsselt
- Die Speicherung von personenbezogenen Daten erfolgt verschlüsselt
- Alle Daten auf mobilen Rechner und Speichermedien werden verschlüsselt
- Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik
- Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert

1.2. Integrität der Systeme und Dienste

1.2.1 Schutz der Datenübertragung

- Einsatz digitaler Signaturverfahren zur Sicherung der Authentizität von Datenübertragungen
- Anbindung von Niederlassungen oder Homeoffice nur über VPN-Verbindungen

1.2.3 Weitere Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste

- Härtungsmaßnahmen werden umgesetzt (z.B. Einschränkung/Deaktivierung nicht notwendiger Berechtigungen, Ports, Protokolle, Server)
- Umsetzung der Mandantentrennung durch Trennung auf Datenebene
- Es erfolgt eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware
- Data Loss Prevention Lösungen werden eingesetzt

1.3. Verfügbarkeit der Systeme und Dienste

1.3.1 Sicherung der Verfügbarkeit personenbezogener Daten

- Regelmäßige Kontrollen des Systemzustandes (Monitoring)

1.3.2 Löschung

- Personenbezogene Daten des Auftraggebers werden nach dessen Weisung, sowie nach Beendigung des Auftrags, vollständig gelöscht, entsprechend der Vorgaben der DSGVO

- Aktenvernichter/-schredder (mind. Stufe 3, cross cuting) für Papierdokumente

1.4 Belastbarkeit der Systeme und Dienste

1.4.1 Absicherung gegen Störungen (Kontinuitätssicherung)

- Virenscanner mit aktuellen Suchmustern (mind. tagesaktuell) auf allen Endgeräten
- Einsatz von Firewall Systemen (z.B. am zentralen Übergang ins Internet, Absicherung von Datenbanken auf Webservern)
- Datenspeicherung in einem RAID-System

1.4.2 Wiederanlauf und Wiederherstellung der Verfügbarkeit

- Geeignete physische Aufbewahrung von Backup-Medien (z.B. Tresor, Feuerschutz, räumliche Trennung)
- Geeigneter Schutz von Backups vor Verschlüsselung durch Ransomware

1.5 Organisatorische Schutzmaßnahmen

1.5.1 Organisatorische Sicherheitsmaßnahmen

- Die Rollen und Verantwortlichkeiten im Bereich der Datensicherheit sind beschrieben, besetzt und intern bekannt
- Sicherheitsrichtlinien für den Umgang mit Informationen sind definiert, von der Geschäftsleitung verabschiedet und den Mitarbeitern kommuniziert
- Awarenessmaßnahmen für alle Anwender bezüglich Datenschutz und Datensicherheit
- Schulungsmaßnahmen bzw. eigene geeignete Fortbildung im Datenschutz
- Regelung zur mobilen/privaten Nutzung von Endgeräten (z.B. Smartphones, Notebooks) durch Mitarbeiter sind getroffen
- Trennung von Produktivsystemen und Entwicklungs-/Testsystemen
- In der Test- und Entwicklungsumgebung werden nur synthetische Daten, also keine Echtdaten oder personenbezogene Daten verarbeitet
- Verbot der Ablage personenbezogener Daten in Source Code (Repositories)

1.5.2 Auftragskontrolle

- Dokumentation aller Auftragsverarbeiter, die für die Verarbeitung der in diesem Vertrag beschriebenen personenbezogenen Daten eingesetzt werden
- Alle relevanten Auftragsverarbeiter verfügen über eine etablierte Zertifizierung im Bereich Informationssicherheit (z.B. ISO 27001, BSI IT-Grundschutz)