Technische und organisatorische Maßnahmen

von edoc solutions ag

Änderungshistorie

Version	Zuständig	Bezeichnung
2018-06-01	edoc	Initiale Erstellung des Dokumentes
2022-05-27	Olbring, ext. DSB	Aktualisierung des Dokumentes nach erneuter Bestandsaufnahme
2023-03-02	Christian Scharf, ISB edoc Olbring, ext. DSB	Aktualisierung des Dokumentes nach erneuter Bestandsaufnahme. Harmonisierung mit TOMs der Cloud-Dienste. Anpassung an edoc CI.
2023-04-04	Christian Scharf, ISB edoc	Anpassung an edoc CI.

Inhaltsverzeichnis

1 Allgemeine Schutzmaßnahmen

1.1 Sicherstellung der Vertraulichkeit

1.1.1 Zutrittskontrolle

1.1.1.1 Beschreibung

Der räumliche Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, ist Unbefugten zu verwehren.

1.1.1.2 Maßnahmen

- Das Unternehmen verfügt über einen zentralen und besetzten Empfangsbereich.
- Ein Zutrittskontrollsystem ist im Unternehmen vorhanden.
- Die Räumlichkeiten des Unternehmens sind stets verschlossen.
- Es existiert eine Zutrittsregelung für betriebsfremde Personen.
- Im Unternehmen ist eine zentrale Schlüsselverwaltung zur Ausgabe von Schlüsseln etabliert.
- An zentraler Stelle wird eine Schlüsselliste geführt, aus der hervorgeht, welcher Mitarbeiter wann einen Schlüssel erhalten hat.
- Besucher erhalten einen Besucherausweis.
- Der Zutritt zu Serverräumen ist auf berechtigte Mitarbeiter beschränkt.
- Serverräume sind stets verschlossen.
- Das Gebäude ist alarmgesichert.
- Eine Gebäudeüberwachung erfolgt durch Videoüberwachung.

1.1.2 Zugangskontrolle

1.1.2.1 Beschreibung

Es ist zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können.

1.1.2.2 Maßnahmen

- Mitarbeiter erhalten individuelle Benutzernamen und Kennwörter für die Anmeldung am PC-Arbeitsplatz.
- Initialkennwörter müssen vom Anwender geändert werden.
- Kennwörter verfügen über Komplexitätsanforderungen (z.B. Zahlen, Buchstaben, Sonderzeichen) und sind ausreichend lang.
- Interne Netze sind gegen unberechtigte Zugriffe von extern durch eine Firewall geschützt.
- Externe Zugriffe auf interne Netze sind ausschließlich über verschlüsselte Verbindungen (z.B. VPN) möglich.
- PC-Arbeitsplätze und Notebooks verfügen über einen Anti-Viren-Schutz.
- E-Mail-Virenschutz über vorgelagerte externe Instanz.
- Trennung von Konten mit User- und Adminrechten in mehreren Ebenen.

1.1.3 Zugriffskontrolle

1.1.3.1 Beschreibung

Es ist zu 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.

1.1.3.2 Maßnahmen

Ein Berechtigungskonzept liegt im Unternehmen vor und enthält differenzierte Berechtigungsstufen.

Über Benutzerprofile ist in den Anwendungen sichergestellt, dass Mitarbeiter ausschließlich zur Aufgabenerfüllung notwendige Rechte erhalten.

Nicht mehr benötigte IT-gestützte Datenträger werden datenschutzgerecht entsorgt.

Die Administration von Servern und Anwendungen ist auf berechtigte Mitarbeiter begrenzt.

1.1.4 Trennungsgebot

1.1.4.1 Beschreibung

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

1.1.4.2 Maßnahmen

- Im Unternehmen wird zwischen Produktiv- und Testsystem unterschieden.
- Daten unterschiedlicher Projekte / Auftraggeber werden, soweit möglich und erforderlich, getrennt verarbeitet.

1.2 Sicherstellung der Integrität

1.2.1 Weitergabekontrolle

1.2.1.1 Beschreibung

Bei einer Weitergabe personenbezogener Daten ist sicherzustellen, dass die Daten während der Übertragung oder des Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.2.1.2 Maßnahmen

- Im Unternehmen stehen Verfahren zu Verfügung, die einen verschlüsselten Austausch personenbezogener Daten ermöglichen
- Anhand organisatorischer Vorgaben werden Mitarbeiter dahingehend verpflichtet, personenbezogene Daten keinesfalls über unsichere oder nicht datenschutzkonforme Dienste auszutauschen

1.2.2 Eingabekontrolle

1.2.2.1 Beschreibung

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

1.2.2.2 Maßnahmen

- Eine Nachvollziehbarkeit von Eingabe, Änderung und Löschung von personenbezogenen Daten ist durch softwareseitige Funktionen im erforderlichen Umfang gegeben.
- Es erfolgt eine eindeutige Auftragsgestaltung.
- Durchführung von Auftragskontrollen.

1.3 Sicherstellung der Verfügbarkeit und Belastbarkeit

1.3.1 Verfügbarkeitskontrolle

1.3.1.1 Beschreibung

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1.3.1.2 Maßnahmen

- Es erfolgt eine redundante Absicherung von Servern und Datenbeständen.
- In den Serverräumen liegt eine angemessene redundante unterbrechungsfreie Stromversorgung (USV) vor.
- Der Serverraum verfügt über redundante Klimaanlagen.
- Der Serverraum verfügt über Rauchmelder.
- Im oder vor den Serverräumen befinden sich Feuerlöscheinrichtungen.
- Datensicherungen werden an einem sicheren, ausgelagerten Ort aufbewahrt.
- Datenrücksicherungen erfolgen regelmäßig durch Testszenarien.
- Virenscanner sind unternehmensweit auf den Endgeräten installiert.
- Virenscanner aktualisieren sich automatisch.
- Betriebssysteme auf Client-Arbeitsplätzen werden regelmäßig aktualisiert.
- Betriebssysteme auf Servern werden regelmäßig aktualisiert.
- Im Unternehmen sind Verfahren implementiert, die eine regelmäßige Aktualisierung auch für Hilfsprogramme (z.B. PDF-Reader, zip-Programme) gewährleisten.
- Die Firewall- und Routersysteme werden regelmäßig aktualisiert (Firmwareupdate).

1.4 Regelmäßige Überprüfung, Bewertung und Evaluierung

1.4.1 Auftragskontrolle

1.4.1.1 Beschreibung

Die Verarbeitung personenbezogener Daten im Auftrag darf nur nach Anweisung des Auftraggebers erfolgen.

1.4.1.2 Maßnahmen

- Die Auswahl von externen Dienstleistern erfolgt unter Anwendung größter Sorgfalt (insbesondere bezüglich des Datenschutzes und der Informationssicherheit).
- Mit externen Dienstleistern, die personenbezogene Daten verarbeiten oder im Rahmen der Tätigkeit einsehen könnten, bestehen vertragliche Regelungen unter Einhaltung der Vorgaben aus Art. 28 der Datenschutzgrund-Verordnung.

- Beim Einsatz externer Dienstleister, die personenbezogene Daten verarbeiten, wird sichergestellt, dass eine Rechtsgrundlage für die Verarbeitung (z.B. Vereinbarung zur Auftragsdatenverarbeitung, EU-Standardvertragsklauseln) gegeben ist.
- Es sind Verfahren implementiert, die sicherstellen, dass personenbezogene Daten nach Auftragsende vernichtet bzw. gelöscht werden. Etwaige gesetzliche Aufbewahrungsfristen werden dabei berücksichtigt und eingehalten.
- In den vertraglichen Regelungen mit externen Dienstleistern werden Kontrollrechte vereinbart.
- Die Vereinbarungen zur Auftragsverarbeitung mit externen Dienstleistern enthalten Regelungen zur Sicherstellung der Vertraulichkeit.

1.4.2 Datenschutzmanagement

1.4.2.1 Beschreibung

Sicherstellung der Etablierung eines angemessenen Datenschutzmanagementsystems

1.4.2.2 Maßnahmen

- Ein externer Datenschutzbeauftragter ist im Unternehmen schriftlich bestellt.
- Ein Informationssicherheitsbeauftragter ist im Unternehmen schriftlich bestellt.
- Mitarbeiter sind schriftlich zur Verschwiegenheit verpflichtet.
- Mitarbeiter werden in regelmäßigen Schulungen bezüglich des Datenschutzes sensibilisiert.
- Im Unternehmen liegt ein dokumentiertes Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs.1 DSGVO) vor. Verarbeitungstätigkeiten im Auftrag werden gem. Art. 30 Abs. 2 DSGVO dokumentiert.
- Im Unternehmen liegt eine Dokumentation der Maßnahmen zur Sicherheit der Verarbeitungstätigkeiten vor (sog. TOM's)
- In regelmäßigen Prüfungen wird sichergestellt, dass die etablierten Maßnahmen zur Einhaltung des Datenschutzes angemessen sind.

2 Ergänzende Schutzmaßnahmen Cloud-Dienste

2.1 Sicherstellung der Vertraulichkeit

2.1.1 Zugriffskontrolle

2.1.1.1 Beschreibung

Es ist zu 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.

2.1.1.2 Maßnahmen

- Zugriff auf Kundendaten nur über API, API-Calls mit Authentifizierung (Secret-Key oder Benutzerauthentifizierung)
- Kundenseitige Rechteverwaltung innerhalb der eigenen Instanz.
- Quellcode liegt in Azure Dev Ops / GIT mit mehrstufigem Verfahren zum Deployment.
- Funktionstrennung bei der Produktivsetzung neuer Versionen.

- Ein Vier-Augen-Prinzip ist über AzureDevOps technisch erzwungen.
- Ausschließlich verschlüsselter Zugriff über definierte Ports.
- Verschlüsselung der Datenträger

2.1.2 Trennungsgebot

2.1.2.1 Beschreibung

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

2.1.2.2 Maßnahmen

- Die Anwendungen erlauben eine logische Mandantentrennung.
- Quellcode liegt in Azure Dev Ops / GIT mit mehrstufigem Verfahren zum Deployment.
- Funktionstrennung bei der Produktivsetzung neuer Versionen.
- Ein Vier-Augen-Prinzip ist über AzureDevOps technisch erzwungen.

2.2 Sicherstellung der Integrität

2.2.1 Weitergabekontrolle

2.2.1.1 Beschreibung

Bei einer Weitergabe personenbezogener Daten ist sicherzustellen, dass die Daten während der Übertragung oder des Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

2.2.1.2 Maßnahmen

- Ausschließlich verschlüsselter Zugriff über definierte Ports.

2.2.2 Eingabekontrolle

2.2.2.1 Beschreibung

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

2.2.2.2 Maßnahmen

- Monitoring auf Anwendungsebene und zugesagte Reaktionszeiten im Rahmen der Wartungsvereinbarungen
- Es finden proaktive Wartungen der bereitgestellten Dienste statt.

2.3 Sicherstellung der Verfügbarkeit und Belastbarkeit

2.3.1 Verfügbarkeitskontrolle

2.3.1.1 Beschreibung

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

2.3.1.2 Maßnahmen

- Daten befinden sich in der Verwaltungshoheit des Kunden. Die Verarbeitung durch edoc erfolgt temporär zusätzlich zur Datenspeicherung im Verantwortungsbereich des Kunden. Eine Speicherung bei edoc erfolgt, sofern im Prozesskontext erforderlich.
- Möglichkeiten zur Kundenseiteigen Datensicherung werden bereitgestellt.