Technische und organisatorische Maßnahmen

Sicherheit der Verarbeitung gem.

Art. 32 DSGVO

der

---

edoc solutions AG

Geltungsbereich: Cloud-Dienste der edoc solutions AG

Änderungshistorie

Version	Zuständig	Bezeichnung
20220224	ssch / comdatis	Initiale Erstellung
20220311	Höltken, Püttmann (beide edoc), Olbring (comdatis)	Abstimmung des TOM-Katalogs und Qualitätssicherung

Inhaltsverzeichnis

1 Sicherstellung der Vertraulichkeit

1.1 Zutrittskontrolle

1.1.1 Beschreibung

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

1.1.2 Maßnahmen

- Das Unternehmen verfügt über einen zentralen und besetzten Empfangsbereich.
- Ein Zutrittskontrollsystem ist im Unternehmen vorhanden, d.h. Türsicherung durch Türöffner, Ausweisleser, Schließautomatik o.ä.
- Im Unternehmen ist eine zentrale Schlüsselverwaltung zur Ausgabe von Schlüsseln etabliert.
- Der Zutritt zu Serverräumen ist auf berechtigte Mitarbeiter beschränkt.
- Serverräume sind stets verschlossen.
- Das Gebäude ist alarmgesichert.

1.2 Zugangskontrolle

1.2.1 Beschreibung

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

1.2.2 Maßnahmen

- Mitarbeiter erhalten individuelle Benutzernamen und Kennwörter für die Anmeldung am PC-Arbeitsplatz.
    - Ausschließlich berechtigte Mitarbeiter haben Zugriff auf die Azure Systeme
    - Zugriff auf Kundendaten nur über API, API-Calls mit Authentifizierung (Secret-Key oder Benutzerauthentifizierung)
    - Kunde verwaltet die Anwenderberechtigungen innerhalb seiner Instanz selber, er kann auf die Konfiguration seiner Software zugreifen. Nicht

jeder Benutzer beim Kunden hat administrative Rechte (keycloak als Drittanbieterlösung).

- PC-Arbeitsplätze werden bei Inaktivität automatisch gesperrt und können nur durch Kennworteingabe wieder entsperrt werden.
- Kennwortvorgaben für Benutzer des Kunden innerhalb der Applikation über AD des Kunden synchronisierbar
- Kennwörter werden verschlüsselt in der Datenbank gespeichert.
- Zugriff auf gespeicherte Fernwartungsinformationen zur Kundenapplikation steht ausschließlich berechtigten Mitarbeitern zur Verfügung.
- edoc nutzt für Administration KEYCLOAK ohne AD-Anbindung für Login für Zugriff auf Service (System Control)
- Zugriff auf Microsoft-Ressourcen für Mitarbeiter der edoc setzt 2-Faktor-Authentifizierung voraus
- Zugriff per RDP bzw. SSH muss zunächst in Azure aktiviert werden (Kurzzeitfreigabe mit automatischem Ablauf)
- AzureDevOps mit mehrstufigem Verfahren zum Deployment:
    - Development
    - Test
    - Quality Assurance
    - Current
- Funktionstrennung bei der Produktivsetzung neuer Versionen, insb. kann ein Entwickler seine Changes nicht selber in die Produktion übernehmen. Ein Vier-Augen-Prinzip ist über AzureDevOps technisch erwzungen.
- Firewall erlaubt Zugriff über Port 80 (redirect zu SSL) bzw. Port 443
- Verschlüsselung auf dem Host mittels Azure Disk Encryption

1.3 Zugriffskontrolle

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.

1.3.2 Maßnahmen

- Nur wenige mit Admin-Rechten in der Umgebung system control
- Quellcode liegt in Azure Dev Ops / GIT
- Funktionstrennung bei der Produktivsetzung neuer Versionen, insb. kann ein Entwickler seine Changes nicht selber in die Produktion übernehmen. Ein Vier-Augen-Prinzip ist über AzureDevOps technisch erwzungen.

1.4 Trennungsgebot

1.4.1 Beschreibung

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden.

1.4.2 Maßnahmen

- Die Anwendungen erlauben eine logische Mandantentrennung (Single Tenant). Der Tenant kann wahlweise auch vom Kunden bereitgestellt werden.
-
- AzureDevOps mit mehrstufigem Verfahren zum Deployment:
    - Development
    - Test
    - Quality Assurance
    - Current

2 Sicherstellung der Integrität

2.1 Weitergabekontrolle

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.

2.1.2 Maßnahmen

- System Control: keine kritische E-Mail-Kommunikation (nur Info zu neuem Benutzer, Info an Buchhaltung, Monitoring)
- Invoice App verschickt E-Mail z.B. eingehende Rechnungen (Workflow-Benachrichtigungen), Systemmails an definierte Postfächer oder Systeme)
- Firewall erlaubt Zugriff über Port 80 (redirect zu SSL) bzw. Port 443
- Sicherstellung des Einsatzes verschlüsselter Verbindungen einschl. Dienste zur Zertifikatsüberwachung

2.2 Eingabekontrolle

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 Maßnahmen

- Sicherstellung der Maschinenverfügbarkeit über Microsoft durch zugesagte SLA
- Monitoring auf Anwendungsebene und zugesagte Reaktionszeiten im Rahmen der Wartungsvereinbarungen
- System Operation zur proaktiven Wartung ist bei bereitgestellten Services der edoc inkludiert. Bei eigenem Kundentenant oder on-prem-Betrieb beim Kunden kann System Operation optional gebucht werden.
-

3 Sicherstellung der Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

3.1.1 Beschreibung

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

3.1.2 Maßnahmen

- Daten befinden sich in der Verwaltungshoheit des Kunden. Die Verarbeitung bei edoc erfolgt temporär, eine Speicherung bei edoc erfolgt – sofern im Prozesskontext notwendig – zusätzlich zur Datenspeicherung im Verantwortungsbereich des Kunden.
- Datensicherungen können in der System Control durch den Kunden aktiviert werden.
- Datensicherung liegen in der Verpflichtung des Kunden, über System Control kann eine Sicherung aktiviert werden.
- Durchführung eigener und regelmäßiger Schwachstellenscans
- Sicherstellung von Updateverfahren für Betriebssysteme auf Servern und Clients
- Sicherstellung von Updateverfahren für Hilfsprogramm (z.B. PDF-Reader)
- Einsatz von Lösungen zum Virenschutz

4 Regelmäßige Überprüfung, Bewertung und Evaluierung

4.1 Auftragskontrolle

4.1.1 Beschreibung

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

4.1.2 Maßnahmen

- Subscription-Modell: Dienst erlischt zum Ende der Vertragslaufzeit, Abschalten der Maschine, Tenant wird gelöscht
- Temporäre Speicherung bei Umgang mit Daten in Verarbeitung (Beleglesung, Workflow)
- Sicherstellung vertraglicher Regelungen (Auftragsverarbeitung, EU-Standardvertragsklauseln)

4.2 Datenschutzmanagement

4.2.1 Beschreibung

Sicherstellung der Etablierung eines angemessenen Datenschutzmanagementsystems

4.2.2 Maßnahmen

- Ein Datenschutzbeauftragter ist im Unternehmen schriftlich bestellt.
- Mitarbeiter werden in Schulungen regelmäßig bezüglich des Datenschutzes sensibilisiert.
- 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.
- Verschwiegenheitsverpflichtungen der Mitarbeiter
- Richtlinien / Arbeitsanweisungen für den Umgang mit Daten und den IT-Systemen, zum Umgang mit Datenpannen und Betroffenenanfragen
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 und Art. 30 Abs. 2 DSGVO

5 Eingesetzte Dienste und Services

Dienst	Zweck	Dienstanbieter	Hosting
Microsoft Azure	Betrieb der Maschinen	Microsoft	Europa
Azure Cognitive Services	Datenextraktion	Microsoft	Europa
Ticketsystem	Betrieb des Ticketsystems	edoc (Eigenentwicklung)	Serverraum der edoc (Weilerswist)