Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Versionshistorie

Datum	Inhalt	Freigabe durch
18.05.2018	Initiale Erstellung der TOMs	Ferdinand Seulen
23.11.2018	Anpassung TOMs gemäß Weiterentwicklung	Ferdinand Seulen

1) Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

a) Zutrittskontrolle

- Schließanlage Büroraume:

  Im täglichen Betrieb ist der Zugang zu den Geschäftsräumen mit Schließzylindertechnik über eine Transponder-Lösung gesichert. Die Transponder werden an Mitarbeiter nur gegen Unterschrift herausgegeben. Bei Verlust werden die Schließsysteme für den Transponder gesperrt, welcher dann für Außenstehende nicht nutzbar ist.

- Zutritt und Überwachung des Rechenzentrums

  Der Zutritt zum Rechenzentrum, in dem die Server betrieben werden, ist mittels biometrischen Fingerabdrucks gesichert. Eine Einbruchmeldeanlage schütz zudem vor unbefugtem Zutritt und benachrichtig im Notfall den 24/7 Sicherheitsdienst, welcher in ständiger Bereitschaft ist. Dies gilt für alle Brandabschnitte.

b) Zugangskontrolle

Die Auftragnehmer stellt durch entsprechende Verfahren und Maßnahmen sicher, dass nur autorisierte Personen Zugang zu den im Eigentum des Auftraggebers stehenden Daten haben. Zur Sicherstellung unbefugter Systembenutzung werden folgende Maßnahmen ergriffen:

- Einrichtung eines Benutzerstammsatzes pro User

  Die Benutzeranlage erfolgt nur mit Freigabe durch den zuständigen Vorgesetzten. Pro Anwendung hat der jeweilige Benutzer nur eine Kennung

- Verschlüsselung von Datenträgern

  Mobile Datenträger und Festplatten von relevanten mobilen PC's (z.B. Laptops) werden unter Verwendung einschlägiger Software verschlüsselt

- Kennwortrichtlinien

  Mindestlänge, regelmäßiger Wechsel, Sonderzeichen, Groß- und Kleinschreibung, keine identischen Passwörter über 5. Generationen.

- Virenscanner- und Firewalls

  Für den Schutz der Server, des Systems und der Daten werden Virenscanner und Firewalls eingesetzt. Mehrere redundante Firewall-Systeme schützen die DMZ und das Intranet. Die Systeme werden täglich direkt von Mitarbeitern überprüft und zusätzlich vollautomatisch überwacht.

c) Zugriffskontrolle

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Differenzierte Berechtigungen und Kenntnisnahme

  Für alle Benutzer werden bei sämtlichen Applikationen Berechtigungen per Antragsformular und Unterzeichnung durch den Vorgesetzten vergeben. Jedem Benutzer werden nur die für seine Arbeitsdurchführung notwendigen Berechtigungen erteilt.

- Zugriffsprotokollierung & Auswertungen

  Auswertungen sind im Verdachtsfall unter Einbeziehung des Datenschutzbeauftragten möglich.

d) Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- "Interne Mandantenfähigkeit“ / Zweckbindung

  Alle Daten der Auftraggeber und Auftragnehmer werden im ERP-System in dem einen vorliegenden Mandanten verarbeitet. Zugriffe haben dadurch nur die berechtigten Mitarbeiter die Auftragnehmer.

- Funktionstrennung / Produktion / Test

  Für die produktiven Dienste bestehen so genannte Drei-Maschinen-Landschaften.

  Auf dem Entwicklungsserver werden die Programme und Geschäftsprozesse entworfen. Der Staging Server dient der Überprüfung der Prozesse und der Daten und der Freigabe zum Transport in die produktive Umgebung. Nur auf dem Produktivserver werden die Daten endgültig verarbeitet und gespeichert.

2) Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- Verschlüsselung /Tunnelverbindung (VPN = Virtual Private Network)

  Zugriffe auf Datenbestände von außerhalb sowie die Übertragung sensibler Daten finden ausschließlich per IPSEC oder SSL Tunnelverbindung statt.

- Protokollierung

  Die Datenverarbeitung und -Weitergabe wird in Transaktionslog-Dateien der

verschiedenen Dienste aufgezeichnet und dokumentiert, zusätzlich kommt ein zentraler Syslog-Server zum Einsatz.

- Transportsicherung

  Alle Datenbestände, die zwecks Datensicherung auf separate Datenbänder gesichert werden, werden verschlüsselt, so dass diese von Fremdsystemen nicht lesbar sind.

b) Eingabekontrolle

Zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind werden verschiedene Prüfsysteme eingesetzt. Die Kontrolle erfolgt per Überprüfung der Transaktionslog-Dateien und der Syslog Protokolle. Schreibvorgänge, die über die Web-Anwendung getätigt werden, werden in einer Datenbank protokolliert und können nachvollzogen werden (Benutzeridentifikation, Transaktionskontrolle). Im zentralen ERP-System werden Änderungen ebenfalls aufgezeichnet und können gezielt ausgewertet werden.

3) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Verfügbarkeitskontrolle

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Backup-Verfahren

  Alle relevanten Daten (Datenbanken, E-Mails, File-Systeme) werden auf separaten Backup Servern gespeichert. Die Datensicherungen werden täglich durchgeführt.

- Spiegeln von Festplatten. z.B. RAID-Verfahren

  Die Daten der Auftragnehmer und der Auftragnehmer-Kunden werden auf Festplatten im RAID-Level 1 gespiegelt verarbeitet. Alle anderen Diensteserver (Mail, File, Portal) werden mit RAID-Level 5 bzw. 1 gespeichert.

- Unterbrechungsfreie Stromversorgung (USV)

  Eine unterbrechungsfreie Stromversorgung mit 60kVA Leistung befindet sich im Rechenzentrum. Die USV garantiert eine Überbrückungszeit sowie das kontrollierte Herunterfahren der kritischen Systeme.

b) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):

- Notfallplan

  Für die Beseitigung von etwaigen Systemausfällen und Störungen existiert ein Notfallplan, welcher aufgrund regelmäßig durchgeführter Disaster Recovery Tests bei Bedarf an die aktuelle Situation angepasst wird.

4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Auftragskontrolle

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer.

- Eindeutige Vertragsgestaltung

  im Dienstleistungsvertrag werden Art und Weise der Auftragsabwicklung festgehalten. In der Regel wird ein Pflichtenheft/ Leistungsbeschreibung als Anlage zum Vertrag erstellt, in dem Beauftragung, Abwicklung, Service Level und involvierte Abteilungen detailliert geregelt sind.

- Formalisierte Auftragserteilung

  Die Beauftragung und der Rücklauf von Informationen zwischen Auftraggeber und Auftragnehmer erfolgt in abgestimmter Form und in der Regel über eine webbasierte Anwendung, Datenschnittstellen oder standardisierte Auftragsformulare.

- Kontrolle der Vertragsausführung

  Für abwicklungsrelevante vertragliche Vorgänge sind nach DIN ISO 9001:2015 Verfahrens- und Arbeitsanweisungen vorhanden. Die Einhaltung wird durch die jeweiligen Vorgesetzten und sogenannte Key User sichergestellt. Eine interne Revisionsabteilung und das Qualitätsmanagement prüfen die Einhaltung der vertraglichen Vereinbarungen.

b) Kontinuierliche Überprüfung und Verbesserung

Es finden in regelmäßigen Abständen Überprüfungen der organisatorischen und technischen Sicherheitsmaßnahmen statt. Ziel ist die kontinuierliche Verbesserung. Regelmäßige Datenschutzschulungen tragen zur zusätzlichen Sicherheit bei.

5) Technische und organisatorischen Umsetzung des Rechts auf Löschung, „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)

Zur Löschung werden Daten auf Wunsch einfach gelöscht, also nicht mehrfach überschrieben. Physische Datenträger mit sensiblen Daten werden geschreddert oder so deformiert, dass ein Auslesen nicht mehr möglich ist.