Technisches und organisatorische Maßnahmen nach Art. 32 DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

- Ein abgestuftes Zutrittskontrollsystem (Schlüssel mit individuellen Zutrittsrechten) schützt vor unberechtigtem Zutritt.
- Zutrittsberechtigungen werden zentral erteilt.
- Die Beantragung der Zutrittsrechte ist nur über den entsprechenden Verantwortlichen möglich.
- Zutritt zu Serverräumen ist nur dem notwendigen Personal gestattet und eingerichtet.
- Es ist eine Gästeregelung implementiert. Dies bedeutet das nichtöffentliche Bereiche nur in Begleitung von Mitarbeitern betreten werden können.

Zugangskontrolle

- Der Schutz der IT-Systeme ist durch Authentifikations- und Autorisierungssysteme (Benutzerkennung und Passwort) gewährleistet.
- Zugangsberechtigungen erfolgen nach dem Minimalprinzip (nur die notwendigen Rechte zur Aufgaben- und Leistungserfüllung).
- Die Vergabe und der Entzug (Deaktivierung) von Benutzerkonten durch die IT erfolgt nur nach schriftlicher Beauftragung der Personalabteilung.
- Bei mehrmaliger Fehleingabe der Zugangsdaten wird das Benutzerkonto gesperrt.
- Die Entsperrung erfordert eine persönliche Authentifizierung des Users und ist nur vom IT Support umsetzbar.
- Der Umgang mit Zugängen und Passwörtern ist verbindlich in Richtlinien geregelt und wird in regelmäßigen Mitarbeiter-Schulungen kommuniziert.
- Die Netzwerksegmentierung trennt Netzwerke verschiedener Sicherheitsstufen mittels Firewalls.
- Es werden Firewall-Systeme genutzt, die fortlaufend auf dem aktuellen technischen Stand gehalten werden.
- Es werden speicherresidente Virenscanner, mit mehrmals täglichem Updates, auf allen Client-Systemen verwendet.
- Die Administration und Überwachung der Virenscanner wird zentral gesteuert.
- Alle Freigaben (z.B. Datei- und Druckerfreigaben), Anwendungseinstellungen und weitere sicherheitsrelevante Einstellungen sind über zentral gesteuerte Richtliniensätze für den Benutzer unveränderlich vorgegeben.
- Der Schutz vor unberechtigtem Einsehen der Büro-Arbeitsplätze ist durch die automatisch startende Sperre (Energiesparmodus) mit Passwortschutz gewährleistet.
- Eine regelmäßige Belehrung der Mitarbeiter zur Notwendigkeit des manuellen Sperrens bei Verlassen des Arbeitsplatzes sorgt für die notwendige Sensibilisierung.
- Software-Installationen werden zentral über den IT Support durchgeführt.
- Anwendungen, die Arbeitsplatzfreigaben ermöglichen, sind nur für vertraglich vereinbarte Wartung durch IT-Dienstleister zugelassen und dürfen nur mit Genehmigung oder im Beisein eines IT-Administrators benutzt werden.

Zugriffskontrolle

- Zugriffsberechtigungen werden nach dem Minimalprinzip erteilt. In den IT-Systemen existiert ein granulares Rechtesystem (d.h. Sicherstellung, dass Daten je nach Recht komplett verborgen, nur angezeigt, veränderbar oder löschbar werden).
- Die Steuerung der Neuanlage von Daten erfolgt über separate Rechte.
- Die Erteilung und Änderung von Zugriffsrechten für die Mitarbeiter ist nur über den entsprechenden Verantwortlichen möglich.
- Die Umsetzung von Löschanforderungen ist in den jeweiligen Prozessabläufen sowie den dazu bestehenden Arbeitsanweisungen und Richtlinien geregelt.
- Funknetzen (WLAN) sind sicher nach dem Stand der Technik verschlüsselt.

Datenträgerkontrolle

- Festplatten werden nach Ausmusterung mit einem definierten Verfahren mehrfach überschrieben (gelöscht).
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden sicher zerstört (geschreddert).

Trennungskontrolle

- Durch die konsequente Rechtevergabe in den verarbeitenden Systemen ist sichergestellt, dass die Mitarbeiter ausschließlich nur auf Daten zugreifen können, die sie für Ihre Arbeitsaufgaben benötigen. Damit ist eine Trennung der Kunden- und Partner-Daten von Daten anderer Auftraggeber oder Eigendaten gewährleistet (Mandantentrennung).
- Die Test- und Entwicklungsumgebungen sind von den Produktivumgebungen getrennt.

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO, Art. 25 Abs. 1 DSGVO)

- Für die Pseudonymisierung ist der Auftraggeber verantwortlich.
- Im Supportfall ist es dem Verantwortlichen möglich eine Datensicherung verschlüsselt auf einen Server des Auftragnehmers zu übertragen. Die Daten sind grundsätzlich nur für den Bearbeiter beim Auftragnehmer einsehbar, der die Datensicherung verarbeitet.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Standardmäßig werden gesicherte Übertragungswege bzw. eine verschlüsselte Kommunikation bei Datenaustausch (insbesondere bei automatisierten Schnittstellen) verwendet.
- Der E-Mail-Verkehr ist nur für den dienstlichen Verkehr zugelassen (organisatorisch in der entsprechenden Richtlinie geregelt).
- Die Versendung von E-Mails mit vertraulichen Daten erfolgt standardmäßig verschlüsselt (diese Anforderung ist in einer Richtlinie geregelt, die Mitarbeiter werden diesbezüglich durch regelmäßige Schulungen sensibilisiert).
- Die Internetnutzung ist durch geeignete Kontroll- und Filtermaßnahmen geregelt.
- Die Verwendung mobiler Datenträger ist durch die entsprechende Richtlinie organisatorisch geregelt.
- Insbesondere werden zur Weitergabe von Daten nur registrierte und verschlüsselte Speichermedien verwendet.

- In Bereichen wo prozessual bedingt externe mobile Datenträger verwendet werden, ist die Einhaltung des Datenschutzes sowie der Datensicherheit durch entsprechende Arbeitsanweisungen gesondert geregelt.

Eingabekontrolle

- Die Verarbeitung personenbezogener Daten im Sinne des Datenschutzes ist durch die konsequente Rechtevergabe in den verarbeitenden Systemen und durch spezielle Arbeitsanweisungen sichergestellt.
- Es erfolgt ein Logging (Anlagedatum, letztes Änderungsdatum, Bearbeiter) in den verarbeitenden Systemen zur Nachvollziehbarkeit von Änderungen.
- Die Auswertungen der Logging-Daten werden nach Datenschutz- und Kundenrichtlinien zentral erstellt.
- Eine Beantragung der Auswertungen ist nur durch den entsprechenden Verantwortlichen möglich.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

- Es existiert ein ständig optimiertes IT-Sicherheitskonzept.
- Die redundante Anbindung sichert die erforderliche Verfügbarkeit der Internetverbindung durch Redundanz.
- Es stehen eigens eingerichtete und abgesicherte Netzwerkbereiche (DMZ's) für Partner mit direkter Anbindung über VPN-Verbindung zur Verfügung.
- Die DMZ's schützen von außen zugängliche IT-Systeme.
- Die Administration und Wartung der IT-Systeme wird durch Verfahren und Prozesse sichergestellt.
- Die Ausfallsicherheit wird durch ein geeignetes Notfallkonzept und die Vorhaltung von Redundanzen gewährleistet.
- Kritische Systeme sind untereinander redundant ausgelegt.
- Eine USV-Anlage dient zum Schutz vor Stromausfällen der Server- und Netzwerkräume.
- Eingesetzte Anwendungssoftware und Betriebssysteme werden durch festgelegte Routinen aktuell gehalten (z.B. sicherheitsrelevante Updates und Fixes).
- Änderungen an Kernsystemen erfolgen erst nach erfolgreichen Prüfungen und Tests auf den Testumgebungen.
- Die datenschutzgerechte Entsorgung von elektronischen Datenträgern (insbesondere Festplatten, USB-Sticks, Speicherkarten, optische Datenträger, Bänder) sowie von Papierdokumenten wird durch ein zertifiziertes Unternehmen durchgeführt.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Ein abgestuftes Verfahren dient der Absicherung gegen Datenverlust und ist durch sekundäre Datenspeicher sowie Datenkopien auf Festplatte und weitere Medien realisiert.
- Die Backup Datenträger werden in einem gesicherten Bereich gelagert.

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

Auftragskontrolle

- Die Datenverarbeitung erfolgt durch eine eindeutige und schriftliche Vertragsgestaltung sowie einer regelmäßigen Kontrolle der Umsetzung.
- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.

Datenschutzmanagement

- Das Datenschutz-Management ist durch Datenschutz-Richtlinien, Arbeitsanweisungen und Prozessbeschreibungen sichergestellt. Diese Dokumente sind für alle Mitarbeiter im Intranet einsehbar.
- Die Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung dienen, werden geprüft.

Incident-Response-Management

- Weiterführende Maßnahmen, Prozesse und Dokumente (z.B. Notfallpläne, Wiederanlaufpläne, Richtlinien) sind im Management System dokumentiert und unterliegen einer ständigen Qualitätskontrolle.

Datenschutzfreundliche Voreinstellungen

- Personenbezogene Datenverarbeitende Systeme und Anwendungen enthalten von den Benutzern nicht änderbare Privacy-by-Default- sowie Privacy-by-Design-Einstellungen