Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

viridicon AG

Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Dokumentation und Auswertung von Beweisen
- Pläne zum Umgang mit erkannten Angriffen und Störungen
- Bewertung von Sicherheitsverletzungen und Systemstörungen
- Meldungsweg für Ereignisse und Schwächen sind sichergestellt
- Risikoangemessene Klassifizierung personenbezogener Daten
- Regelung der erlaubten Handhabung und Nutzung von Datenträgern
- Untersagung der betriebliche Nutzung privater Geräte (BYOD)
- Regelung der Umstände der zulässigen Privatnutzung betrieblicher Mittel
- Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt
- Leitungsebene wird regelmäßig über Status von Datenschutz und Informationssicherheit sowie mögliche Risiken und Konsequenzen aufgrund fehlender Maßnahmen informiert
- Bestellung eines Informationssicherheitsbeauftragten
- Regelmäßige interne Kontrolle der Sicherheitsmaßnahmen
- PDCA-Zyklus
- Bestellung eines Datenschutzbeauftragten
- Zuständigkeiten für Datenschutz und Informationssicherheit sind definiert
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.
- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogen und mindestens halbjährlich evaluiert wird.
- Die an Mitarbeiter ausgegebene Schlüssel, Zugangskarten oder Codes sowie im Hinblick auf die Verarbeitung personenbezogener Daten erteilte Berechtigungen, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten eingezogen, bzw. entzogen.
- Mitarbeiter werden im Hinblick auf den Datenschutz auf Verschwiegenheit verpflichtet, belehrt und instruiert, als auch auf mögliche Haftungsfolgen hingewiesen. Sofern Mitarbeiter außerhalb betriebsinterner Räumlichkeiten tätig werden oder Privatgeräte für betriebliche Tätigkeiten einsetzen, existieren spezielle Regelungen zum Schutz der Daten in diesen Konstellationen und der Sicherung der Rechte von Auftraggebern einer Auftragsverarbeitung.
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).

- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.

Zutrittskontrolle

- Regelungen bezüglich Dienstleistern und Dritten (z.B. Reinigungs- und Wartungsdiensten)
- Sicherung auch außerhalb der Arbeitszeit z.B. durch Sicherheitsdienst
- Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen
- Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im Safe
- Abgestufte Sicherheitsbereiche und kontrollierter Zutritt
- Verschließen von Türen und Fenstern außerhalb von Geschäftszeiten
- Regelmäßige Überprüfung und Wartung der Anlagen
- Anweisung zur Ausgabe von Schlüsseln
- Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)
- Gesondert gesicherte abschließbare Serverräume
- Einbruchmeldeanlagen / Alarmanlage
- Einbruchschutzeinrichtungen (z.B. Einfriedungen oder einbruchsichere Schlösser, Fenster u. Türen, Absichern von Schächten, etc.)
- Sicherheitsschlösser
- Beaufsichtigung von Hilfskräften
- Videoüberwachung
- Dauerhaft Personal anwesend
- Wachpersonal
- Fenstersicherung
- Chipkarten-/Transponder-Schließsystem
- Zutrittsregelungen für betriebsfremde Personen

Zugangskontrolle / Zugriffskontrolle

- Die erneute Verwendung bereits genutzter Passworte wird unterdrückt (Passworthistorie)
- Sichtschutz von Bildschirmarbeitsplätzen und von mobil verwendeten Notebooks
- Regelmäßige Auswertung von Protokollen (Logfiles)
- Protokollierung von Zugriffen auf Daten
- Protokollierung von Dateilöschungen
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
- Intrusiondetection (IDS)
- Software für das Security Information und Event Management (SIEM)
- Umgesetzte Clean Desk Policy
- Intrusionprevention (IPS)
- SPAM-Filter
- Protokollierung und Auswertung der Systembenutzung
- Virenscanner (Clients und Server)
- Verpflichtung zur Vertraulichkeit von Lieferanten
- Protokollierung von Dateizugriffen
- Verpflichtung zur Vertraulichkeit von Mitarbeitern
- Geregelter Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- Geregelter Prozess zum Rechteentzug bei Aufgabenänderung von Mitarbeitern
- Geregelter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Verwendung von individuellen Passwörtern, auch initial
- Hashing von gespeicherten Passwörtern
- Verhinderung von Trivialpasswörtern (z.B. Hund1, Hund2, Hund3)
- Mindestens 8 Ziffern / Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)
- Zwei-Faktor-Authentifizierung
- Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- Bildschirmsperre
- Vernichtung von Festplatten
  Festplatten werden über die Firma Schmitt-Recycling nach DIN 66399 Sicherheitsstufen O-3 / T-3 / E-2 / H-5 (Partikelgröße 11,5 x 26 mm) zerstört. Die in den Partikeln enthaltenen Stoffe, werden der Wiederverwertung zugeführt

- Berechtigungs-/ Authentifizierungskonzepte mit auf Nötigste beschränkten Zugriffsregulierungen
- Richtlinie zum Einsatz von USB-Sticks
- Einsatz von zentraler Smartphone-Administrations-Software
- Stets aktuelle Softwareversionen
- Stets aktueller Virenschutz
- Firewall (Hardware)
- Einsatz von VPN-Technologie
- Verschlüsselung von Festplatten (FileVault, Bitlocker)
- Mindestpasswortlängen und Passwortmanager
- Authentifikation mit Benutzer und Passwort und bei erhöhtem Schutzbedarf durch eine zusätzliche Multifaktor-Authentisierung
- Ordnungsgemäße Vernichtung von Datenträgern
- Verschlüsselung von mobilen Datenträgern und Geräten
- Firewall (Software)
- Einsatz von Intrusion-Detection-Systemen

Weitergabekontrolle

- Festlegung und Dokumentation der Empfänger
- E-Mail-Verschlüsselung (PGP)
- Verschlüsselung von Datenträgern und Verbindungen
- E-Mail-Verschlüsselung (S/MIME)
- Möglichkeit zur Pseudonymisierung von Testdaten
- verschlüsselter Remotezugriff
- VPN-Verbindung (IP-Sec)
- S/MIME oder PGP
- E-Mail Versand mit verschlüsseltem Anhang
- Datenaustausch über https-Verbindung
- Verschlüsselung mobiler Datenträger (z.B. USB, externe Festplatten, Speicherkarten, usw.), die Daten des Verantwortlichen enthalten
- Verschlüsselung von Laptopfestplatten
- Übergreifende Regelung zur Datenübertragung
- Gesicherter Eingang für An- und Ablieferung von Daten
- Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle
- Festlegung der Bereiche, in dem sich Datenträger befinden müssen
- Sicherungskopien von Datenträgern, die transportiert werden müssen
- Datenträgerentsorgung - Sicheres Vernichten von Datenträgern: Vernichtung nach DIN 66399 Sicherheitsstufe P5 / H5
- Regelung zur Anfertigung von Kopien

Eingabekontrolle

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Differenzierte Benutzerberechtigungen
- Protokollierung von Dateneingaben-, Änderungen und Löschungen
- Kennzeichnung erfasster Daten
- Festlegung von Benutzerberechtigungen (Profile)
- Organisatorische Festlegung von Eingabezuständigkeiten
- Protokollierung von Eingaben/Löschungen
- Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke
- Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)
- Protokollauswertungssystem
- Über OS-Standard hinausgehendes Log-Konzept
- Dedizierter Logserver

Auftragskontrolle

- Kontrolle der Einhaltung bei Auftragnehmern
- Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten
- Schriftliche Festlegung der Weisungen
- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Erfassung vorhandener Unterauftragsverarbeiter (einheitliches Vertragsmanagement)
- Regelmäßige Kontrollen beim Unterauftragsverarbeiter
- Vor-Ort-Kontrollen beim Unterauftragsverarbeiter
- Überprüfung des Datensicherheitskonzepts beim Unterauftragsverarbeiter
- Sichtung vorhandener IT-Sicherheitszertifikate der Unterauftragsverarbeiter
- Geregelter Auswahlprozess
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Verfügbarkeitskontrolle / Integrität

- Durchführung von Belastbarkeitstests
- Ausreichende performante Wiederherstellungsmöglichkeiten
- Dokumentation der Systeme
- Sicherheit der Verkabelung (Datenleitung/ Stromleitung/ Telekommunikationsleitung)
- Kapazitätsmessung
- Geplante Instandhaltung von Systemen (Wartungsliste)
- Identifikation der IT-Geräte, Assets und Netzwerksysteme in der Infrastruktur der Organisation.
- Periodische Trainings und Sensibilisierungskampagnen innerhalb der Organisation in den Bereichen Datenschutz und Informationssicherheit
- Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates
- Systemhärtung (Deaktivierung nicht erforderlicher Dienste und Komponenten)
- Durchführung von Penetrationstests
- Datenspeicherung auf RAID-Systemen (RAID 1 und höher)
- Redundante Klimatisierung
- Redundante USV-Anlage
- Redundante Stromversorgung
- Ausweich-Rechenzentren oder anderweitiges Ersatzsystem vorhanden (Hot- bzw. ColdStand-by?)
- Einbeziehung des Einflusses angrenzender baulicher Einrichtungen
- Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)
- Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)
- Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten
- Notfallkonzept
- Einsatz von Festplattenspiegelung
- Sicherstellung einer funktionsfähigen Klimatisierung
- Unterbrechungsfreie Stromversorgung und Überspannungsschutz
- Ständig kontrolliertes Backup- und Recoverykonzept
- Rauchmelder in Serverräumlichkeiten
- Brandmeldeanlagen in Serverräumlichkeiten
- Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten
- Serverräumlichkeiten in separatem Brandabschnitt
- Unterbringung von Backupsystemen in separaten Räumen und Brandabschnitten
- USV-Anlage (Unterbrechungsfreie Stromversorgung)
- Netzersatzanlage

- Klimatisierte Serverräumlichkeiten
- Wassersensoren in Serverräumlichkeiten
- Löschwasserschutz der Server
- Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)
- Aufstellungsort des Backupsystems in getrenntem Brandabschnitt
- Art des Backupmediums: Tape
- Art des Backupmediums: Veam
- Art des Backupmediums: Externe Festplatte
- Art des Backupmediums: NAS
- Volles Backup
- Differentielles Backup
- Das Backup geht mehrere Generationen zurück
- Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft
- Bestehen eines Rücksicherungskonzept
- Regelmäßige und gesteuerte Überprüfung der Backupwiederherstellbarkeit
- Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal
- Erfassung und Dokumentation von IT Systemen und Anwendungen
- Vereinbarung bzgl. Übergabe der (Daten-) Sicherunge

Gewährleistung des Zweckbindungs-/Trennungsgebotes

- Trennung von Produktiv- und Testsystem
- Zertifizierung nach ISO27001
- Richtlinien und Arbeitsanweisungen für die Mitarbeiter
- Datensicherungen der Daten des Verantwortlichen auf separaten Datenträgern ohne Daten weiterer Kunden
- Datensicherungen der Daten des Verantwortlichen auf separaten Datenträgern ohne Daten weiterer Kunden
- Verarbeitungen der Daten des Verantwortlichen und der Daten anderer Kunden durch unterschiedlichen Mitarbeitern des Auftragsverarbeiters
- Dateiseparierung bei Datenbanken
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
- Trennung von Entwicklungs-, Test- und Produktivsystem
- Logische Mandantentrennung (Software)
- Funktionstrennung
- Berechtigungskonzept, das der getrennten Verarbeitung von Daten unterschiedlicher Kunden Rechnung trägt.
- Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)