Technische und organisatorische Maßnahmen (TOM) bei seca

Darstellung der technischen und organisatorischen Maßnahmen bei seca gemäß Art. 32 DSGVO.

Anmerkung: seca betreibt ein Informationssicherheitsmanagementsystem mit integriertem Datenschutzmanagement gemäß der ISO/IEC 27001 + ISO/IEC 27701 und strebt die eine zeitnahe Zertifizierung nach den genannten Normen an.

A. Pseudonymisierung und Verschlüsselung (Art. 32 (1) (a) DSGVO)

Kryptographie

- Benutzung von E-Mail-Verschlüsselung (TLS 1.2) und sicheren Verfahren zum Nachrichtenaustausch
- Sichere Schlüsselverwaltung
- Anonymisierung bzw. Pseudonymisierung bei der Verarbeitung von Studiendaten
- Pseudonymisierung in Logdateien

B. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 (1) (b) DSGVO)

Organisation der Informationssicherheit

- Verwendung einer zentralen Software für die Smartphone-Administration
- Möglichkeit des ferngesteuerten Löschens von Daten auf den Mobilgeräten
- Verwendung einer zentralen Software für die Smartphone-Administration
- Möglichkeit des ferngesteuerten Löschens von Daten auf den Mobilgeräten

Personalsicherheit

- Verpflichtung der Mitarbeiter auf die Richtlinien zu Datenschutz und Informationssicherheit
- Clean-Desk-Richtlinie und Clear-Screen-Richtlinie
- regelmäßige Schulungen zu Datenschutz und Informationssicherheit, u.a. zum Phishing und zum Umgang mit unbenutzten Geräten und zur Abmeldung von Service, welche nicht länger genutzt werden und zum Umgang mit Authentisierungsinformationen, Schlüsseln und Transpondern

Verwaltung der Werte

- Registrierung der IT-Ausrüstung
- Dokumentation der Ausgabe und Rückgabe der IT-Ausrüstung
- Richtlinie zur Dokumentenlenkung mit der Festlegung von Vertraulichkeitsstufen und entsprechende Kennzeichnung der Dokumente
- Beauftragung von Aktenvernichtern mit Datenschutzsiegel zur Vernichtung von Akten und elektronischen Datenträgern

Zugangssteuerung

- Implementierung einer Richtlinie für die Zugangsvergabe nach einem Rechte-Rollen-Modell
- Matrix zur Zuweisung von Benutzerprofilen zu IT-Systemen
- Rechtevergabe nach dem "Need to know"-Prinzip
- formalisierter Prozess für der Rechtevergabe mit Einholung der Genehmigung durch den jeweiligen Vorgesetzten
- Löschen des Benutzers bzw. Entzug der Benutzerrechte beim Verlassen des Unternehmens
- Anpassung der Benutzerrechte bei Wechseln der Verantwortung
- Single-Sign-On-System für alle wesentlichen Anwendungen
- Lese-/Schreibrechte-Konzepte für Laufwerke und Dateien sowie einzelne Seiten und Bereiche im internen Wiki
- Lese-/Schreibrechte-Konzepte für Ticketsysteme
- zentrale Verwaltung der Rechte über den Verzeichnisdienst Microsoft Active Directory
- Passwort-Richtline einschließlich Passwortlänge, Komplexität, Historie, Gültigkeit
- Notwendigkeit, ein initiales Passwort bei der ersten Anmeldung zu ändern
- Vergabe von zusätzlichen Benutzerkonten für Administratoren (zusätzlich zu deren persönlichem Benutzerkonto)
- grundsätzlich keine Domänen- oder lokale Administratorrechte für Benutzer (Ausnahme: lokale Administratorrechte für Rechner in einem speziell abgeschotteten Entwickler-Netzwerk)
- mit Transponder gesicherter Zugang zu Druckern und individuelle Druckerwarteschlangen
- Protokollierung von fehlerhaften Anmeldeversuchen

- Sperrung des Benutzerkontos bei Überschreitung der maximalen Anzahl von Fehlversuchen
- Konsequenter Einsatz von Zweifaktor-Authentifizierung für alle Benutzer
- Einschränkung der Benutzung von Applikationen durch PC-Management
- Zugang zu Quellcode von Programmen in der Abteilung Research & Development nur für die Entwickler

Physische und umgebungsbezogene Sicherheit

- Alarmsystem für besonders sensible Bereiche (einschließlich Serverräume)
- Videoüberwachung des Zutritts zu besonders sensiblen Bereichen
- Schutz durch Bewegungsmelder und Lichtschranken
- während der Geschäftszeiten besetzte Rezeption im Eingangsbereich
- Aufzeichnung der Besuche externer Personen (Besucherliste und Ausweise)
- Begleitung der Besucher durch Mitarbeiter auf dem Werksgelände
- mitarbeiterspezifische Zutrittsberechtigung über Transponder-Schließsystem
- Platzierung der Serverräume an besonders ausgewählten Orten zum Schutz vor unbefugtem Zugang, Wasser- oder Feuerschaden, Blitzschlag usw.
- Platzierung der redundanten Serverräume in unterschiedlichen Gebäuden
- Kenntnis von der Existenz und der Aktivität in besonders sensiblen Bereichen (einschließlich Serverräume) nach dem "Need to know"-Prinzip
- besonders sensible Bereiche sind nicht als solche erkennbar und nicht direkt von außen zugänglich
- Zutritt Externer zu Serverräumen nur mit Begleitung
- Klimatisierung und Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuerlöscher und Feuermeldeanlage
- physisch geschützte Verlegung der Kabel
- Verschlossene Verteilerschränke bzw. -räume in besonderen Bereichen
- Verschrottung von Datenträgern generell über spezialisierten Dienstleister

Kommunikationssicherheit

- Benennung von Zuständigen für das Netzwerk und Einbindung eines ausgewählten Dienstleisters zur Netzwerk-Administration
- strenge Regeln für die Vergabe von Rechten zum Zugang zu Netzwerken und Netzwerkdiensten
- konsequente Verwendung von Firewalls mit VPN-Technologie
- kontinuierliches Logging und Monitoring der Netzwerkaktivitäten
- Begrenzung der im Netzwerk integrierten Systeme
- Separates Entwicklernetz
- WLAN-Netz für verschiedene Zwecke (z.B. separates Gäste-WLAN)

Anschaffung, Entwicklung und Instandhalten von Systemen

- Entwicklung von Software für selbst genutzte Anwendungen nach den gleichen Standards und Prozessen wie für Medizinsoftware
- etablierter Change-Control-Prozess auch für selbst genutzte Anwendungen
- Prozesse zur Verifizierung und Validierung extern und selbst entwickelter Applikationen
- Besonders geschütztes Netzwerk für die Entwicklung von Produkten und selbst genutzten Applikationen
- Besonders geschützte Testumgebung
- Generierung von speziellen Testdaten anstelle echter Datensätze mit personenbezogenen Daten

Dienstleister- und Lieferantenbeziehungen

- Sorgfältige Auswahl des Sicherheits- und Reinigungspersonals
- Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DSGVO bei Datenverarbeitung im Auftrag bzw. bloßen Datenschutzklauseln und Geheimhaltungsvereinbarungen bei der sonstigen Beauftragung von Dienstleistern und Lieferanten

C. Rasche Wiederherstellung der Verfügbarkeit und des Zugangs (Art. 32 (1) (c) DSGVO)

Betriebssicherheit

- Monitoring von Ressourcen
- Regelmäßige Löschung veralteter Daten zur Speicherplatzoptimierung
- Außerbetriebsetzung von Anwendungen, Systemen, Datenbanken oder Umgebungen, wenn der Anwendungszweck entfällt
- Optimierung von Batch-Prozessen und Zeitplänen
- Bandbreitenbegrenzung ressourcenintensive Dienste (z. B. Video-Streaming)
- Trennung von Entwicklungs-, Test- und Betriebsumgebungen bei Clouddiensten, internen Anwendungen und Systemen

- Webfilter und Sperrung von Downloads
- Konsequente Verwendung von Virenschutzsoftware
- Abonnement der einschlägigen Warn- und Informationsdienste
- Prozess zur Datensicherung nach dem Generationenprinzip und regelmäßiger Test der Backups auf Wiederherstellbarkeit
- Aufbewahrung eines Teils der Datensicherungen an einem externen Ort
- Audit-Log bei den relevanten, unternehmensweit genutzten Systemen
- Change-Management und Genehmigungsverfahren bei der Aktualisierung der Applikationen
- Prüfung der Applikationen vor der Installation auf einem Testsystem
- Einsatz von Rollback-Strategien bei der Aktualisierung der Applikationen

Informationssicherheitsaspekte beim Business Continuity Management

- Richtlinie zum Business Continuity Management
- Notfall-Internetzugang über einen zweiten Provider
- Unterbrechungsfreie Stromversorgung (USV)

D. Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit (Art. 32 (1) (d) DSGVO)

- Regelmäßige Überprüfung, Bewertung und Evaluierung im Rahmen des Informationssicherheitsmanagementsystems (ISMS)
- Fachliche Durchführung durch den Informationssicherheitsbeauftragten, welcher unabhängig von der IT und den anderen Fachabteilungen direkt an die Geschäftsführung berichtet

Handhabung von Datenschutz- und Informationssicherheitsvorfällen

- Prozess zur Behandlung von Datenschutz- und Informationssicherheitsvorfällen

Compliance

- Betreuung von Datenschutz und Informationssicherheit durch die hauseigene Rechtsabteilung

Auftragskontrolle (Einbezug Dritter / Outsourcing)

- Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung nach Art. 28 DSGVO bzw. EU-Standardvertragsklauseln bei Drittlandsbezug (Art. 44 ff DSGVO)
- Regelungen zum Einsatz weiterer Sub-Auftragsverarbeiter

Maßnahmen im Zusammenhang mit Cloud Services

- seca betreibt SaaS-Services ausschließlich auf der Infrastruktur des auf externes Server-Hosting spezialisierten Sub-Auftragsverarbeiters Amazon Web Services EMEA SARL (AWS) am Standort Frankfurt am Main (für Kunden innerhalb der EU/EWR).
- seca verschlüsselt sämtliche personenbezogenen Daten in den SaaS-Services, so dass ein unberechtigter Zugriff auf diese Daten ausgeschlossen ist.
- Das Schlüsselmanagement erfolgt durch seca.