Technische und organisatorische Maßnahmen (TOM)

Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

PROZESS- UND VERFAHRENSÜBERGREIFENDE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DER EKOM21 – KGRZ HESSEN

1. PSEUDONYMISIERUNG

- Definition von Maßnahmen zur Pseudonymisierung erfolgen abhängig von Verarbeitungstätigkeit

2. VERSCHLÜSSELUNG

- Transportverschlüsselung im WAN21 der ekom21 als kundenspezifische Zusatzleistung
- Technische Richtlinie Transportverschlüsselung
- Verschlüsselung mit Storage-Technologien gemäß Technischer Handlungsanweisung Storage
- Verschlüsselung der Daten auf Clients
- Hashs der Passworttabellen im Verzeichnisdienst

3. GEWÄHRLEISTUNG DER VERTRAULICHKEIT

ORGANISATIONSKONTROLLE

- ISO 27001 Zertifizierung auf Basis von IT-Grundschutz
- Richtlinien und Handlungsanleitungen zum Datenschutz und zur IT-Sicherheit
- schriftl. bestellte/r behördliche/r Datenschutzbeauftragte/r und Vertreter/in
- regelmäßige DS Schulungen aller Mitarbeiter/innen
- Datenschutzmanagement
- Verpflichtung aller Mitarbeiter/innen auf das Datengeheimnis
- Regelmäßige IT-Sicherheitsschulungen für die Mitarbeiter

ZUGANGSKONTROLLE

- Überwachung des Gebäudes durch Alarmanlage (außerhalb der Geschäftszeiten und dauerhaft für einzelne Bereiche), Maßnahmen bei Verlust der Codekarte
- Einsatz eines Zugangskontrollsystems unter Verwendung von RFID-Chips mit Protokollierung und Maßnahmen bei Verlust eines Chips
- Videoüberwachung von einzelnen Notausgangstüren bei Bewegung
- Verwendung von Mitarbeiterausweisen mit Foto
- Organisationsverfügung Dienstausweis KGRZ
- Einsatz eines Schließsystems für Gebäude und Geschäftsräume
- Videoüberwachung in den Serverräumen des Rechenzentrums bei Bewegung und der Außenbereiche der Notausgänge des Rechenzentrums
- Nutzung eines zentralen Empfangsbereichs mit Besetzung während der Geschäftszeiten, weitere Zu- und Ausgänge über alarmgesicherte Notausgänge
- Bewegungsmelder im RZ-Bereich, Serverraum und teilweise vor Fluchttüren
- Unterbringung RZ, Maschinenraum und Serverräume im Keller
- Isolierverglasung der Fenster und Außenjalousien, im Standort Kassel Panzerglas im Erdgeschoss
- Besucherüberwachung durch Begleitung von Mitarbeitern, Besucherausweise (sichtbar tragend) und Führen eines Besucherbuchs
- Wartung der Geräte durch externe Techniker erfolgt in Begleitung autorisierten Personals und nur nach vorhergehender Anmeldung
- Sicherheitsschlösser und separater Schließkreis für Schlösser RZ-/Serverraum-Türen
- Zentrale Schlüsselverzeichnisse je Standort mit Maßnahmen bei Verlust des Schlüssels

- Reinigung der Räume durch externe Dienstleister während der Arbeitszeit
- Organisationsverfügung Zutritts- und Zugangsregelungen des Unternehmensverbundes KGRZ/ekom21
- Organisationsverfügung Dienstausweis KGRZ

BENUTZERKONTROLLE

- Prozess für Benutzerverwaltung im Verzeichnisdienst
- Identifikation per User-ID und Passwort auf Clients und Servern
- Sperrung des Zugriffs bei Nichteinhaltung der Passwortregeln
- IT-Sicherheitsleitlinie für ekom21 - KGRZ Hessen
- Richtlinie Identity Management
- Richtlinie für IT-Systeme und Netze der ekom21 - KGRZ Hessen
- Organisationsverfügung-Beantragung Änderung von Zulassungen der Kunden zu DV-Systemen
- Operative Handlungsanweisung Überprüfung AD

ZUGRIFFSKONTROLLE

- Zugriffsregelung für Verfahren gemäß Formular „Antrag auf Verfahrenszugang“
- Innerhalb der ekom21 Verwendung komplexer Passwörter im Verzeichnisdienst mit begrenzter Gültigkeitsdauer (<2 Monate) gemäß Richtlinie Identity Management mit Systemprüfung
- Passwörter für Ausnahmefälle und deren Nutzung werden gesondert dokumentiert und in einem geschlossenen Umschlag im Tresor verwahrt, Neukonfiguration nach Gebrauch
- Berechtigungskonzept auf Verzeichnisdienstebene
- Technische Handlungsanweisung Security Gateways
- Protokollierung auf Netzwerkebene
- Protokollierung der AD Benutzerzugriffe auf Betriebssystemebene
- Richtlinie Monitoring und Protokollierung
- System- und Datenbankadministrationskonzept mit abgestuften Administrationsrechten
- Vier-Augen-Prinzip für besondere Administratoren (Firewall, Core Switche)
- Protokollierung von Administrationstätigkeiten, Auswertung der Protokolle bei Bedarf
- Verfahrensspezifisches Berechtigungskonzept der Anwendung

EINGABEKONTROLLE

- Schriftliche Regelungen der Befugnisse zur Eingabe, Kenntnisnahme, Veränderung und Löschung von Daten gemäß Formular „Antrag auf Verfahrenszugang“
- Technische Realisierung der Zugriffsberechtigungen für Programminstallation, Programmausführung, Lesen, Schreiben und Löschen von Dateien im File-System sowie Datenbanken
- Protokollierung der Auf-/Abbau von VPN-Verbindungen, Zugriffe der Benutzer auf Fachverfahren, versuchte Richtlinienverstöße im Verzeichnisdienst, Auswertung nur bei Bedarf
- Richtlinie Monitoring und Protokollierung
- Handlungsanleitung Monitoring und Protokollierung
- Verfahrensspezifische Protokollierung der Zugriffe mittels Server-Logfiles
- Verarbeitungstätigkeitsabhängige Maßnahmen zur Eingabekontrolle

SPEICHERKONTROLLE

- Verwendung von Festplatten, Magnetbändern und CD-ROM/WORM

DATENTRÄGERKONTROLLE

- Schriftliche Regelungen zum Einsatz von Datenträgern und Datenträgerkopien
- Aufbewahrung von Datenträger im Robotersystem und in Sicherheitsbereich
- Entfernung von vollen Datenträgern aus Bereichen
- Dokumentation der Datenträger und Bestandskontrolle (Robotersystem)

- Tägliche Protokollierung des Entfernens von Datenträgern
- Auswertung der Protokolle für Datenträger
- Tägliche Anfertigung von Voll- bzw. Änderungssicherungen
- Regelungen zur Datenträgerentsorgung und deren Protokollierung
- Richtlinie datenschutzgerechte Datenträgerentsorgung
- Handlungsanleitung datenschutzgerechte Datenträgerentsorgung
- Nutzung externer Datenträgerentsorgung
- Schriftliche Auftragsvergabe für externe Datenträgerentsorgung
- Regelungen für den Versand von Datenträgern, Transport durch Bote/Kurier/fester Taxifahrer gesichert in einem Transportkoffer, Dokumentation durch Rückgabeschein und Begleitschein

AUFTRAGSKONTROLLE

- Benutzungsordnung der ekom21 KGRZ Hessen
- Strukturierte Erfassung der Lieferanten und Kunden, Prüfung auf Umgang mit Daten
- Individuelle Verträge zur DV im Auftrag
- Individuelle Verträge zur Fernwartung
- Handlungsanleitung DV im Auftrag
- Besichtigung von Räumlichkeiten von Auftragnehmern
- Prüfung des Sicherheitskonzeptes von Auftragnehmern

TRANSPORTKONTROLLE

- Übertragung von Daten zu Kunden über Standleitung oder VPN (verschlüsselt)
- Technische Richtlinie Transportverschlüsselung
- Einsatz einer Firewall
- VPN Verbindung mit IPSec und dedizierter Firewall, Einzelplatzverbindungen mit 2 Faktor-Authentifizierung (OTP, e-Token)
- Protokollierung von Datenübertragungen auf Netzebene, Auswertung der Protokolle bei Bedarf

ÜBERTRAGUNGSKONTROLLE

- Fernwartungskonzept zur Fernwartung von Software und Anwendungen
  - Überwachung der Remote Sessions
  - Fernaufschaltung über spezielle Anwendung inkl. Authentifizierung
  - Systemadministrator vor Ort (Vier-Augen-Prinzip)
  - Protokollierung der Fernwartung
  - Auswertung der Protokolle im Verdachtsfall

TRENNUNGSKONTROLLE

- Getrennte Verarbeitung und Speicherung von Daten für unterschiedliche Zwecke (Verfahren und Mandanten). Verarbeitungstätigkeitsabhängige logische und/oder physikalische Trennung
- Trennung der DV-Anlagen und Datenträger für besonders sensible Daten physikalisch (Gesamtsystem) und logisch (Anwendung)

4. GEWÄHRLEISTUNG DER INTEGRITÄT

ZUGANGSKONTROLLE

- Maßnahmen der Zugangskontrolle zur Gewährleistung der Vertraulichkeit

EINGABEKONTROLLE

- Maßnahmen der Eingabekontrolle zur Gewährleistung der Vertraulichkeit
- Verhinderung von unbefugten Eingaben durch Sperrung des Eingabebildschirms nach 15 Minuten

SPEICHERKONTROLLE

- Maßnahmen der Speicherkontrolle zur Gewährleistung der Vertraulichkeit

- Handlungsanleitung generelles Datensicherungskonzept
- Redundanz von Hard- und Software sowie der Infrastruktur gemäß der verarbeitungsspezifischen technischen und organisatorischen Maßnahmen
- Technische Richtlinie Storage
- Technische Handlungsanleitung Storage

DATENINTEGRITÄT

- Funktionstest von neuen oder geänderten Verfahren gemäß Richtlinie für Patch- und Änderungsmanagement der ekom21 – KGRZ Hessen und Handlungsanleitung Change-Management

AUFTRAGSKONTROLLE

- Maßnahmen der Auftragskontrolle zur Gewährleistung der Vertraulichkeit

5. GEWÄHRLEISTUNG DER VERFÜGBARKEIT

ORGANISATIONSKONTROLLE

- Maßnahmen der Organisationskontrolle zur Gewährleistung der Vertraulichkeit
- Leistungsschein Bereitstellung Infrastruktur
- Vertretungsregelungen in IT Operations

ZUGANGSKONTROLLE

- Maßnahmen der Zugangskontrolle zur Gewährleistung der Vertraulichkeit

AUFTRAGSKONTROLLE

- Maßnahmen der Auftragskontrolle zur Gewährleistung der Vertraulichkeit

SPEICHERKONTROLLE

- Maßnahmen der Speicherkontrolle zur Gewährleistung der Vertraulichkeit
- Handlungsanleitung generelles Datensicherungskonzept
- Redundanz von Hard- und Software sowie der Infrastruktur gemäß der verarbeitungsspezifischen technischen und organisatorischen Maßnahmen
- Technische Richtlinie Storage
- Technische Handlungsanleitung Storage

WIEDERHERSTELLBARKEIT

- Richtlinie für Patch- und Änderungsmanagement der ekom21 – KGRZ Hessen
- Handlungsanleitung Change-Management
- Notfallhandbuch (inkl. Wiederanlaufpläne für ASP Anwendungen, Dienste, Netze, Server und Datenbanken)
- Replikat der Datensicherung in anderem Standort (als Rechenzentrum)
- Einsatz von USVs und Brandmelder
- Brandkonzept

ZUVERLÄSSIGKEIT

- System-Monitoring (24x7) durch Command Center inkl. Eskalationsprozess
- Handlungsanweisung Antivirenservice
- Dokumentation von Tests und Freigaben von neuen oder geänderten Verfahren in einem Change Management System gemäß Richtlinie für Patch- und Änderungsmanagement der ekom21 – KGRZ Hessen und Handlungsanleitung Change-Management

6. GEWÄHRLEISTUNG DER BELASTBARKEIT DER SYSTEME

- Redundanz von Hard- und Software sowie der Infrastruktur gemäß der verarbeitungsspezifischen technischen und organisatorischen Maßnahmen
- Technische Richtlinie Storage
- Technische Handlungsanleitung Storage
- Servicebeschreibung Rechenzentrum
- Jährliche Notfalltests im Bereich Technik im Rahmen des Notfallmanagements BSI

- Jährliche Notfalltests für Verfahren im ASP-Betrieb im Rahmen des Notfallmanagements BSI
- Penetrationstest für einzelne Verfahren

7. VERFAHREN ZUR WIEDERHERSTELLUNG DER VERFÜGBARKEIT PERSONENBEZOGENER DATEN NACH EINEM PHYSISCHEN ODER TECHNISCHEN ZWISCHENFALL

- Notfallhandbuch (inkl. Wiederanlaufpläne für ASP Anwendungen, Dienste, Netze, Server und Datenbanken)
- Notfallhandbuch Storage
- Technische Handlungsanweisung im Command Center zur Wiederherstellung der Verfügbarkeit von Verfahren
- Eskalationsprozedur und Kundenkommunikation gemäß Leistungsschein Bereitstellung Infrastruktur

8. VERFAHREN REGELMÄßIGER ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

- Black Building Test durch IT Operations inkl. Evaluierung
- Funktionstests nach gemäß Richtlinie für Patch- und Änderungsmanagement der ekom21 – KGRZ Hessen
- Penetrationstests für einzelne Verarbeitungen siehe verarbeitungsspezifische technische und organisatorische Maßnahmen
- Jährlicher externer Audit der Storage Infrastruktur
- Jährliche Rezertifizierung gemäß ISO 27001 Grundschutz
- Jährliche Notfalltests im Bereich Technik im Rahmen des Notfallmanagements BSI
- Jährliche Notfalltests für Verfahren im ASP-Betrieb im Rahmen des Notfallmanagements BSI
- Regelmäßige Erstellung von Testumgebungen aus Sicherungen für verschiedene Verfahren
- Monatliche Tests der Netzersatzanlage in den Standorten
- Datenschutzmanagement
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle

9. SCHRIFTLICHE DOKUMENTATIONEN

INTERNE VERHALTENSREGELN
☒ Ja ☐ Nein

- o Unternehmenshandbuch
- o Handlungsanleitung Datenschutz Management

RISIKOANALYSE
☒ Ja ☐ Nein

- o Schwellwertanalyse,
- o Datenschutzfolgenabschätzung

DATENSICHERHEITSBESCHREIBUNG
☒ Ja ☐ Nein

- o Verarbeitungstätigkeitsübergreifende Technische und organisatorische Maßnahmen

DATENSICHERHEITSKONZEPT
☒ Ja ☐ Nein

- o ISO 27001 Grundschutz Zertifizierung
- o IT-Sicherheitsleitlinie

WIEDERANLAUFKONZEPT
☒ Ja ☐ Nein

- o Notfallhandbuch

ZERTIFIKAT
☒ Ja ☐ Nein

- o Zertifizierungsstelle: BSI