

**VERARBEITUNGSÜBERGREIFENDE TECHNISCHE UND ORGANISATORISCHE
MAßNAHMEN DER EKOM21 – KGRZ HESSEN****1. DATENMINIMIERUNG****PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME**

- Reduzierung von erfassten Attributen der betroffenen Personen
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Implementierung automatischer Löschroutinen abhängig von der Verarbeitungstätigkeit

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen

2. GEWÄHRLEISTUNG DER VERTRAULICHKEIT**A. VERTRAULICHKEIT****PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME**

- Spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Rechenzentrum der ekom21)
- Schutz vor äußeren Einflüssen (Spionage, Hacking)
- Trennung der DV-Anlagen und Datenträger für besonders sensible Daten physikalisch (Gesamtsystem) und logisch (Anwendung)
- Alarmanlage (außerhalb der Geschäftszeiten und dauerhaft für einzelne Bereiche)
- Zugangskontrollsystem (Verwendung von Transponder mit Protokollierung)
- Videoüberwachung von einzelnen Notausgangstüren bei Bewegung
- Videoüberwachung in den Serverräumen des Rechenzentrums bei Bewegung und der Außenbereiche der Notausgänge des Rechenzentrums
- Sicherheitsschlösser
- Unterteilung in Sicherheitszonen (separater Schließkreis für Schlösser RZ-/Serverraum-Türen)
- Schlüsselregelung (Zentrale Schlüsselverzeichnisse je Standort mit Maßnahmen bei Verlust des Schlüssels)
- Einsatz eines Schließsystems für Gebäude und Geschäftsräume
- Schließsystem mit Transponder
- Schließsystem mit Codesperre
- Ausweispflicht (Mitarbeiterausweis mit Foto)
- Personenkontrolle (Besucherüberwachung durch Begleitung von Mitarbeitern, Besucherausweise (sichtbar tragend) und Führen eines Besucherbuchs)
- Bewegungsmelder im RZ-Bereich, Serverraum und teilweise vor Fluchttüren
- Einbruchhemmende Fenster und Türen
- Auf Datenschutz verpflichtetes Personal
- Festgelegte Reinigungszeiten (Reinigung der Räume durch externe Dienstleister während der Arbeitszeit)
- Beaufsichtigung von Wartungstätigkeiten externer Techniker durch autorisiertes Personal (
- Benutzerkonto für jeden Mitarbeiter
- Passworrichtlinie
- Authentifikation mit Passwort
- Authentifikation über Verzeichnisdienste

- Regelungen beim Ausscheiden von Mitarbeitern
- Sperren der Bootkonfiguration (BIOS, UEFI)
- Automatische Abmeldevorgänge
- Kontensperrung nach mehrmaliger Falscheingabe des Passworts (Verzeichnisdienst)
- Aufteilung der Administratorrechte unter verschiedenen Personen
- Vergabe von Administratorrechten an minimale Anzahl Personen
- Differenzierung administrativer Aufgaben (System- und Datenbankadministrationskonzept mit abgestuften Administrationsrechten)
- Datenträgerverschlüsselung (Clients)
- Datenträgervernichtung nach DIN 66399
- Einsatz von Firewalls
- Datenkommunikation über VPN-Tunnel (Übertragung von Daten zu Kunden über Standleitung oder VPN)
- Einzelplatzverbindungen mit 2 Faktor-Authentifizierung (OTP, e-Token)

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen)
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz
- ISO 27001 Zertifizierung auf Basis von IT-Grundschutz
- Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept) für Transportverschlüsselung
- Richtlinien und Handlungsanleitungen zur IT-Sicherheit (u.a. Leitlinie IT-Sicherheit, Richtlinie Identity Management, Richtlinie IT Systeme und Netze)
- Verpflichtung aller Mitarbeiter/innen auf das Datengeheimnis
- Regelmäßige IT-Sicherheitsschulungen für die Mitarbeiter
- Maßnahmen bei Verlust des Transponders
- Organisationsverfügung Zutritts- und Zugangsregelungen des Unternehmensverbundes KGRZ/ekom21
- Organisationsverfügung Dienstausweis KGRZ
- Unterbringung von RZ und Maschinenraum im Keller
- Standortabhänge Unterbringung von Serverräumen im Keller bzw. anderen Etagen
- Fernwartungskonzept zur Fernwartung von Software und Anwendungen
 - Überwachung der Remote Sessions
 - Fernaufschaltung über spezielle Anwendung inkl. Authentifizierung
 - Systemadministrator vor Ort (Vier-Augen-Prinzip)
- Technische Richtlinie Transportverschlüsselung
- Regelungen für den Versand von Datenträgern, Transport durch Bote/Kurier/fester Taxifahrer gesichert in einem Transportkoffer, Dokumentation durch Rückgabeschein und Begleitschein
- Regelungen zur Datenträgerentsorgung und deren Protokollierung (Richtlinie datenschutzgerechte Datenträgerentsorgung)
 - Nutzung externer Datenträgerentsorgung
 - Schriftliche Auftragsvergabe für externe Datenträgerentsorgung
- Operative Handlungsanweisung Überprüfung AD
- Nutzung eines zentralen Empfangsbereichs mit Besetzung während der Geschäftszeiten, weitere Zu- und Ausgänge über alarmgesicherte Notausgänge

- Technische Handlungsanweisung Security Gateways
- Differenzierung administrativer Aufgaben
- Vier-Augen-Prinzip für besondere Administratoren (Firewall, Core Switches)
- Schriftliche Regelungen der Befugnisse zur Eingabe, Kenntnisnahme, Veränderung und Löschung von Daten gemäß Formular „Antrag auf Verfahrenszugang“
- Organisationsverfügung Beantragung und Änderung von Zulassungen der Kunden zu DV-Systemen
- Arbeiten mit individuellen Benutzerkennungen (Identity Management)

B. PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Transportverschlüsselte Datenübertragung (im WAN21 der ekom21 als kundenspezifische Zusatzleistung)
- Einsatz von selbstverschlüsselnden Festplatten mit Kryptochip
- Verschlüsselung der Daten auf Clients der ekom21

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Technische Richtlinie Transportverschlüsselung
- Technische Handlungsanleitung Transportverschlüsselung

3. GEWÄHRLEISTUNG DER VERFÜGBARKEIT

A. VERFÜGBARKEIT

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Sicherungs- und Wiederherstellungskonzept
- Automatisiertes Anfertigen von Datensicherungen
- Aufbewahrung der Datensicherung in einem anderen Ort
- Festgelegte Zuständigkeiten für die Datensicherung
- Aufbewahren von Datenträgern in gegen Elementarschäden gesicherten Behältnissen (Serverschrank)
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Redundanz von Hard- und Software sowie Infrastruktur abhängig von der Verarbeitungstätigkeit (generelle Datenspiegelung (RAID), überwiegend virtuelle Server, gespiegelte Speichersysteme für einige Systeme)

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Servicebeschreibung Rechenzentrum
- System-Monitoring (24x7) durch Command Center inkl. Eskalationsprozess
- Handlungsanleitung und Richtlinie Monitoring und Protokollierung
- Handlungsanleitung generelles Datensicherungskonzept
- Regelmäßiger Test der Datenwiederherstellung gemäß Technische Richtlinie Datensicherung
- Schriftliche Regelungen zum Einsatz von Datenträgern und Datenträgerkopien
- Meldewege und Notfallpläne
- Aufbewahrung von Datenträgern im Sicherheitsbereich
- Penetrationstests für einzelne Verfahren

B. BELASTBARKEIT VON SYSTEMEN UND DIENSTEN

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Lastausgleich (load balancing) der Netzwerkkomponenten
- Automatische Skalierung virtueller Systeme
- Unterbrechungsfreie Stromversorgung (redundant auf 2 getrennten Wegen)

- Überspannungsschutz
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen
- Feuerlöscher / automatisches Löschesystem
- Brandmelder
- Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung
- IT-Komponenten verfügen über erforderliche Leistungsfähigkeit
- Schutz vor Wassereintrich
- Schutz vor Hochwasser
- Automatisches Notrufsystem

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Technische Richtlinie Storage und Technische Handlungsanleitung Storage

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

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Sicherungs- und Wiederherstellungskonzept
- Notfallplan zur Wiederinbetriebnahme von Servern und Diensten (Notfallhandbuch (inkl. Wiederanlaufpläne für ASP Anwendungen, Dienste, Netze, Server und Datenbanken)
- Notfallplan bei Kompromittierung oder Datenverlust
- Eskalationsprozedur und Kundenkommunikation gemäß Leistungsschein Bereitstellung Infrastruktur
- Technische Handlungsanweisung im Command Center zur Wiederherstellung der Verfügbarkeit von Verfahren
- Eskalationsprozess und Kundenkommunikation gemäß Leistungsschein Bereitstellung Infrastruktur

4. GEWÄHRLEISTUNG DER INTEGRITÄT

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Einsatz von Virenschutzlösungen
- Verschlüsselung der Internetpräsenz
- Überwachen und Protokollieren von Fernwartungsaktivitäten
- Schutz vor äußeren Einflüssen (Spionage, Hacking) durch ein Intrusion Detection System
- Web Application Firewall (für einzelne Verarbeitungen)
- Packet Filter Firewall
- Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste
- Regelung zum Umgang mit mobilen Datenträgern
- Protokollierung der Datenübertragung auf Netzebene
- Protokollierung der AD Benutzerzugriffe auf Betriebssystemebene
- Verhinderung von unbefugten Eingaben durch automatische Sperrung des Eingabebildschirms nach einer vordefinierten Zeitspanne

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Dokumentierte Zuweisung von Berechtigungen und Rollen für Verfahren
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften
- Auswertung von Protokollen bei Bedarf

5. GEWÄHRLEISTUNG DER NICHTVERKETTUNG

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Es werden individuelle Maßnahmen für die einzelnen Verarbeitungstätigkeiten ergriffen

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Getrennte Verarbeitung und Speicherung von Daten für unterschiedliche Zwecke (Trennung durch Verfahren und Mandanten)

6. GEWÄHRLEISTUNG DER TRANSPARENZ

A. TRANSPARENZ

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Protokollierung von Administrationstätigkeiten, Auswertung der Protokolle bei Bedarf
- Protokollierung der Auf-/Abbau von VPN-Verbindungen, Zugriffe der Benutzer auf Fachverfahren, versuchte Richtlinienverstöße im Verzeichnisdienst, Auswertung nur bei Bedarf

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Datenschutzmanagement
- regelmäßige DS Schulungen aller Mitarbeiter/innen
- Dokumentation von Verarbeitungstätigkeiten und -prozessen (Inventarisierung)
- Dokumentation der Verträge mit den intern Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
- Satzung der ekom21 KGRZ Hessen und Entgelt- und Leistungsverzeichnis als anderes Rechtsinstrument im Sinne von Art. 28 Abs. 3 DS-GVO für Auftragsverarbeitung
- Individuelle Verträge zur Auftragsverarbeitung
- Strukturierte Erfassung der Lieferanten und Kunden, Prüfung auf Umgang mit Daten
- Individuelle Verträge zur Fernwartung
- Dokumentation von Widersprüchen
- Dokumentation der Quellen von Daten (je Verarbeitungstätigkeit) und des Umgangs mit Datenpannen
- Benachrichtigung von Verantwortlichen und ggf. Betroffenen bei Datenpannen oder Weiterverarbeitungen zu einem anderen Zweck
- Nachverfolgbarkeit der Aktivitäten als verantwortliche Stelle zur Gewährung der Betroffenenrechte
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten als Verantwortlicher an Betroffene

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

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Automatisierte Auswertung der Protokolldaten
- Protokollierung der Datenträgervernichtung
- Videoüberwachung bei Zutritt zur Datenverarbeitungsanlage
- Dokumentation der Übergabeprozesse bei physischem Transport von Datenträgern
- Protokollierung des Zutritts zu Datenverarbeitungsanlagen oder Räumen in denen Datenverarbeitung stattfindet
- Protokollierung der sicheren Löschungen von Datenträgern
- Stichprobenartige Überprüfung der Wirksamkeit bestimmter Maßnahmen

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Datenschutz-Produktüberprüfung
- Audit/Prüfungen durch den DSB der ekom21
- Incident-Response-Management
- Besichtigung von Räumlichkeiten von Auftragnehmern
- Prüfung des Sicherheitskonzeptes von Auftragnehmern
- Periodische Überprüfung der Verarbeitungstätigkeiten und deren Technischer und organisatorischer Maßnahmen
- Jährliche Überwachung der Zertifizierung gemäß ISO 27001 Grundschutz
- Jährlicher externer Audit der Storage Infrastruktur
- Jährliche Notfalltests im Bereich Technik im Rahmen des Notfallmanagements BSI
- Jährliche Notfalltests für Verfahren im ASP-Betrieb im Rahmen des Notfallmanagements BSI
- Monatliche Tests der Netzersatzanlage in den Standorten
- Regelmäßige Prüfung auf Schwachstellen der IT-Sicherheit mit Bericht an die Geschäftsführung
- Regelmäßige Erstellung von Testumgebungen aus Sicherungen für verschiedene Verfahren
- Auswertung der Protokolle für Datenträgersicherungen

7. GEWÄHRLEISTUNG DER INTERVENIERBARKEIT**PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME**

- Es werden individuelle Maßnahmen für die einzelnen Verarbeitungstätigkeiten ergriffen

ORGANISATORISCHE UND PERSONELLE PROZESSE

- schriftl. bestellte/r behördliche/r Datenschutzbeauftragte/r und Vertreter/in
- Single Point of Contact für Datenschutzfragen
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen