VERARBEITUNGSSPEZIFISCHE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DER EKOM21 – KGRZ HESSEN FÜR DEN VERARBEITUNGSPROZESS

Bereitstellung der Digitalisierungsplattform „civento" für die Erstellung und den Betrieb von Prozessen zur elektronischen Vorgangsbearbeitung

GEWÄHRLEISTUNG DER DATENMINIMIERUNG

Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)

Datenschutzfreundliche Voreinstellungen (Art 25 Abs. 2 DSGVO)

Ebene personenbezogene Daten

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen

Ebene technische Systeme und Dienste

- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten (civento Rechte und Rollenkonzept)

Ebene technische, organisatorische und personelle Prozesse

- Festlegung automatisierter Löschzyklen

GEWÄHRLEISTUNG DER VERTRAULICHKEIT

Vertraulichkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung (Art. 5 Abs. 1 lit. f), Art. 28 Abs. 3 S. 2 lit. b), Art. 29, Art. 32 Abs. 1 lit. b), Art. 32 Abs. 4, Art. 38 Abs. 5 DSGVO)

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

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

Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d), Art. 34 Abs. 2 DSGVO)

Ebene personenbezogene Daten

- Protokollierung lesender Zugriffe

Ebene technische Systeme und Dienste

- Einschränkung von lesenden Zugriffsrechten auf IT-Systeme
- Regelmäßige Passwortwechsel
- Authentifikation mit Passwort
- Authentifikation über Verzeichnisdienste
- Kontensperrung nach mehrmaliger Falscheingabe des Passworts
- Logische Mandantentrennung
- Trennung von Produktiv- und Testsystem
- Transportverschlüsselte Datenübertragung

Ebene technische, organisatorische und personelle Prozesse

- Implementierung eines sicheren Authentisierungsverfahrens
- Durchführung eines Penetrationstests

GEWÄHRLEISTUNG DER VERFÜGBARKEIT

Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)
Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, Art. 34 Abs. 2 DSGVO)

VERFÜGBARKEIT

Ebene personenbezogene Daten

- Einschränkung von Lösch- und Veränderungsrechten

Ebene technische Systeme und Dienste

- Hardwareredundanz
- Dokumentation der Syntax der Daten
- Automatisches Benachrichtigungssystem bei Ausfall

Ebene technische, organisatorische und personelle Prozesse

- Vertretungsregelungen für abwesende Mitarbeitende
- Reparaturstrategien und Ausweichprozesse

BELASTBARKEIT VON SYSTEMEN

Ebene technische Systeme und Dienste

- Lastausgleich (load balancing) der Server
- Lastausgleich (load balancing) der Dienste

Ebene technische, organisatorische und personelle Prozesse

- Penetrationstest

MAßNAHMEN ZUR WIEDERHERSTELLUNG DER VERFÜGBARKEIT PERSONENBEZOGENER DATEN NACH EINEM PHYSISCHEN ODER TECHNISCHEN ZWISCHENFALL

Ebene technische, organisatorische und personelle Prozesse

- Wiederanlaufplan für Verfahren

GEWÄHRLEISTUNG DER INTEGRITÄT

Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)

Integrität (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. f DSGVO)

Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 i. V. m. ErwGr. 71 DSGVO)

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

Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, Art. 34 Abs. 2 DSGVO)

Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DSGVO)

Ebene personenbezogene Daten

- Einschränkung von Schreib- und Änderungsrechten
- Protokollierung von schreibenden/ ändernden Zugriffen
- Protokollierung geänderter Daten

Ebene technische Systeme und Dienste

- Einschränkung von schreibenden Zugriffen und Konfigurationsmöglichkeiten auf IT Systemen
- Differenzierte Berechtigungen für unterschiedliche Transaktionen
- Plausibilitätskontrollen bei der Datenverarbeitung

Ebene technische, organisatorische und personelle Prozesse

- Geordnete und dokumentierte Zuweisung von Berechtigungen und Rollen
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen

GEWÄHRLEISTUNG DER NICHTVERKETTUNG

Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

Ebene personenbezogene Daten

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen

Ebene technische Systeme und Dienste

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten

Ebene technische, organisatorische und personelle Prozesse

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen

GEWÄHRLEISTUNG DER TRANSPARENZ

Transparenz für betroffene Personen (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DSGVO)

Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DSGVO)

Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DSGVO)

Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO)

TRANSPARENZ

Ebene personenbezogene Daten

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen

Ebene technische Systeme und Dienste

- Dokumentation der Bestandteile der Verarbeitungstätigkeit (Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, genutzte IT-Systeme, Betriebsanläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten)
- Versionierung

Ebene technische, organisatorische und personelle Prozesse

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen

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

Ebene technische Systeme und Dienste

- Protokollierung der Anmeldevorgänge
- Protokollierung der Datenzugriffe
- Protokollierung von Löschvorgängen
- Protokollierung der Datenübertragung über Schnittstellen
- Protokollierung der Eingabe bei der Erhebung und Ergänzung von Daten
- Protokollierung der Veränderung oder Korrektur von gespeicherten Daten
- Protokollierung von Konfigurationsänderungen

GEWÄHRLEISTUNG DER INTERVENIERBARKEIT

Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DSGVO)

Identifizierung und Authentifizierung (Art. 12 Abs. 6 DSGVO)

Berichtigungsmöglichkeit von Daten (Art. 5 lit. d, Art. 16 DSGVO)

Löschbarkeit von Daten (Art. 17 Abs. 1 DSGVO)

Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DSGVO)

Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO)

Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DSGVO)

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DSGVO)

Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO)

Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 lit. f und lit. j DSGVO)

Ebene personenbezogene Daten

- Schaffung notwendiger Datenfelder, z.B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

Ebene technische Systeme und Dienste

- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem

Ebene technische, organisatorische und personelle Prozesse

- Es werden ausschließlich verarbeitungsübergreifende Maßnahmen ergriffen