Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend die OZG-Verwaltungsleistung:

„Breitband-Portal“

Zwischen dem Leistungsbezieher (Auftraggeber/Kommune) und dem Leistungserbringer (Auftragnehmer/Kommunalvertreter NRW) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsvereinbarung (nachstehend „Einzel-AV“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung(en) „Breitband-Portal“ als Anlage 1 geschlossen.

Präambel

Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien geschlossenen Rahmenvereinbarung zur Auftragsverarbeitung (nachstehend „**Rahmen-AV**“) die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „Breitband-Portal“.

1 OZG-Verwaltungsleistungs-spezifische Datenkategorien, Zwecke, Betroffene

Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Breitband-Portal“ die folgenden personenbezogenen Daten:

I. Zwecke

- Digitale Antragsstellung und die Genehmigung einer Leitungsverlegung nach § 127 Abs. 1, 2, 3, 6, 7, 8 TKG

II. Betroffene

- Antragssteller (Beschäftigte des Telekommunikationsunternehmens oder seiner Dienstleister)
- Beschäftigte des Wegebaulastträger
- Beschäftigte weiterer Koordinierungsstellen im Rahmen der Zustimmung nach § 127 Abs. 1, 2, 3, 6, 7, 8 TKG
- Beschäftigte bei den Trägern öffentlicher Belange

III. Datenkategorien

Daten zum Antragsteller (Beschäftigte des Telekommunikationsunternehmens, im Folgenden: TK-Unternehmen oder seiner Dienstleister, der im Auftrag des TK-Unternehmens arbeiten)

- Name und Vorname des Antragstellers (Beschäftigte des TK-Unternehmens oder seiner Dienstleister)
- Dienstliche E-Mail-Adresse und dienstliche Tel. Nr. des Antragstellers (Beschäftigte des TK-Unternehmens oder seiner Dienstleister)
- Organisation/Abteilung/Funktion des Antragstellers (Beschäftigte des TK-Unternehmens oder seines Dienstleisters)
- Dienstliche postalische Adresse des Antragstellers (Beschäftigte des TK-Unternehmens oder seiner Dienstleister)
- Daten im Rahmen der Anmeldung, Authentisierung und Autorisierung für die Nutzung des ELSTER-Unternehmenskontos:
- Name der Organisation
- Organisationsanschrift (Straße, Hausnummer, Adresszusatz, PLZ, Ort, Ortsteil, Land)
- Rechtsform

- Registernummer
- Registerart
- Registergericht
- ELSTER-Account-ID
- ELSTER- DUEbEL-ID
- Vertrauensniveau der Identifizierung im Registrierungsfall
- Vertrauensniveau der Authentifizierung im Fall eines Logins
- Identifizierungstyp
- Personentyp (natürliche oder juristische Person)
- Tätigkeit (Information über den Tätigkeitsbereich einer Person)

Weitere Daten im Antrag des Antragstellers und/oder in der Zustimmung des Wegebaulastträgers

- Aktenzeichen/Referenzkennnummer/Vertragsnummer
- Name und Vorname des Beschäftigten weiterer Koordinierungsstellen im Rahmen der Zustimmung nach § 127 Abs. 1, 2, 3, 6, 7, 8 TKG
- Dienstliche E-Mail-Adresse und dienstliche Tel. Nr. des Beschäftigten weiterer Koordinierungsstellen im Rahmen der Zustimmung nach § 127 Abs. 1, 2, 3, 6, 7, 8 TKG
- *Daten von den Beschäftigten der Träger öffentlicher Belange*
- Name und Vorname des Beschäftigten von den Trägern öffentlicher Belange (z.B. Wasser- und Naturschutzbehörde)
- Dienstliche E-Mail-Adresse und dienstliche Tel. Nr. des Beschäftigten der Träger öffentlicher Belange
- *Daten zum Bearbeiter der Genehmigung der Leitungsverlegung nach § 127 Abs. 1, 2, 3, 6, 7, 8 TKG (Beschäftigte des Wegebaulastträgers)*
- Name und Vornamen des Beschäftigten des Wegebaulastträgers
- Dienstanschrift (Straße, Hausnummer, Adresszusatz, PLZ, Ort, Ortsteil, Land)
- Dienstliche E-Mail-Adresse des Beschäftigten des Wegebaulastträgers
- Amt/Dienststelle
- Dienstliche Tel. Nr. und Fax-Nr. des Beschäftigten des Wegebaulastträgers
- Nummer des Dienstzimmers
- civento-Instanz
- Name des civento-Prozesses
- Mandant und Organisationseinheit
- Nutzername/User-ID

Technische Daten, die bei Aufruf der „civento-Plattform“ verarbeitet werden

- Vorgangsart (Name der OZG-Leistung)
- Vorgangs-ID und automatisch generierte ID, die miteinander verknüpft werden
- Eingangsdatum
- Session Cookies
- Serverlogfiles
- Name der abgerufenen Webseite
- Datei, Datum und Uhrzeit des Abrufs
- Übertragene Datenmenge
- Meldung über erfolgreichen Abruf
- Browsertyp nebst Version
- Betriebssystem des Nutzers
- Referrer-URL (die zuvor besuchte Seite)
- IP-Adresse

2 Technische und organisatorische Maßnahmen (TOM)

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die ekom21 mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Für die Bestimmung geeigneter TOM ist zunächst der Schutzbedarf der zu verarbeitenden personenbezogenen Daten festzulegen und hier zu dokumentieren.

Es gelten die TOM in ihrer jeweils aktuellen Fassung:

- Verarbeitungsübergreifende technische und organisatorische Maßnahmen der ekom21 (ekom21-TOM), www.ekom21.de/AVV
- Verarbeitungsspezifische technische und organisatorische Maßnahmen für die Digitalisierungsplattform civento (civento-TOM), www.ekom21.de/AVV

Stand 14.11.2024:

Verfahrensübergreifende technische und organisatorische Maßnahmen der ekom21:

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)

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

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)

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 physisch (Gesamtsystem) und logisch (Anwendung)
- Alarmanlage (außerhalb der Geschäftszeiten und dauerhaft für einzelne Bereiche)
- Zutrittskontrollsystem (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
- Passwortrichtlinie
- 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, zentrale Datensicherungssysteme, zentrale SAN-Systeme)
- 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)

<u>ORGANISATORISCHE UND PERSONELLE PROZESSE</u>

- 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 auf das Datengeheimnis
- Regelmäßige IT-Sicherheitsschulungen für die Mitarbeite
- 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)
- 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
- Handlungsanweisung Security Gateways
- Differenzierung administrativer Aufgaben
- Vier-Augen-Prinzip für besondere Administratoren (Firewall, Core Switche)
- 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)
- Dienstvereinbarung mobiles Arbeiten
- Richtlinie zum Informationsaustausch

PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

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

ORGANISATORISCHE UND PERSONELLE PROZESSE

- Richtlinie Transportverschlüsselung
- Handlungsanleitung Transportverschlüsselung

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

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 Anwendungen
- Spiegelung der Datensicherung und NAS Systeme nach Gießen

ORGANISATORISCHE UND PERSONELLE PROZESSE

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

BELASTBARKEIT VON SYSTEMEN

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Lastausgleich (load balancing) der Netzwerkkomponenten
- Automatische Skalierung virtueller Systeme
- Unterbrechungsfreie Stromversorgung (redundant auf 2 getrennten Wegen(jeder Weg abgesichert durch USV und Netzersatzanlage))
- Überspannungsschutz
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen
- Feuerlöscher / automatisches Löschsystem
- Brandmelder
- Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung

- IT-Komponenten verfügen über erforderliche Leistungsfähigkeit
- Schutz vor Wassereinbruch
- Schutz vor Hochwasser
- Automatisches Notrufsystem

ORGANISATORISCHE UND PERSONELLE PROZESSE

Richtlinie Storage und Handlungsanleitung Storage

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
- Handlungsanweisung im Command Center zur Wiederherstellung der Verfügbarkeit von Verfahren
- Eskalationsprozess und Kundenkommunikation gemäß Leistungsschein Bereitstellung Infrastruktur

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)

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

GEWÄHRLEISTUNG DER NICHTVERKETTUNG

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

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)

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

PERSONENBEZOGENE DATEN UND TECHNISCHE SYSTEME

- Protokollierung von Administrationstätigkeiten, Auswertung der Protokolle bei Bedarf
- Protokollierung des Auf-/Abbaus 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
- Dokumentation von Verarbeitungstätigkeiten und -prozessen (Inventarisierung)
- Dokumentation der Verträge mit den internen Mitarbeitern, 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

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 und in den Räumen der 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 der Technischen und Organisatorischen Maßnahmen
- Jährliche Überwachung der Zertifizierung gemäß ISO 27001 Grundschutz
- Regelmäßige externe Audits
- 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 Netzersatzanlagen
- 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

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)

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

Verarbeitungsspezifische technische und organisatorische Maßnahmen für die Digitalisierungsplattform civento (civento-TOM)

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

3 Liste der genehmigten Subunternehmer

Es gelten die Liste der genehmigten Subunternehmer in ihrer jeweils aktuellen Fassung:

- Die Liste ist einsehbar unter folgendem Link www.ekom21.de/AVV

	Name des Subunternehmers	**Anschrift**	**Leistung**
	Unterauftragnehmer, die im Rahmen aller civento-Prozesse eingesetzt werden		
1	saascom GmbH	Heidelbergerstraße 6 64283 Darmstadt	Softwareentwicklung und -pflege

2	Devoteam GmbH	Gutenbergstraße 10 64331 Weiterstadt	Umsetzung, Design, Support und Fernwartung der Digitalisierungsprojekte auf Basis der Prozessplattform „civento“
3	Strange Consult GmbH	Herzogstandstraße 5 82327 Tutzing	Umsetzung, Design, Support und Fernwartung der Digitalisierungsprojekte auf Basis der Prozessplattform „civento“
4	govITconsult GmbH	Udenborner Straße 17a 34590 Wabern	Umsetzung, Design, Support und Fernwartung der Digitalisierungsprojekte auf Basis der Prozessplattform „civento“
5	Govconsult GmbH	Kesslaustraße 29 76187 Karlsruhe	Erstellung von Statistiken
6	msg systems AG	Robert-Bürkle-Str. 1 85737 Ismaning	Prozessanalyse, Prozessdesign, Prozessmodellierung und Unterstützungsleistungen im Projektmanagement im Rahmen der OZG- Leistungen
	Unterauftragnehmer, die im Rahmen von civento-Prozessen eingesetzt werden, die die Softwarekomponente „Biometrieprüfung“ beinhalten		
7	Bundesdruckerei GmbH	Kommandantenstraße 18 10969 Berlin	Betrieb und Wartung der Softwarekomponente „Biometrieprüfung“
	Unterauftragnehmer, die im Rahmen von civento-Prozessen eingesetzt werden, die Antragsdaten mithilfe von Fit-Connect übermitteln		
8	FITKO (Föderale IT-Kooperation)	Zum Gottschalkhof 3 60594 Frankfurt am Main	Übermittlung von Antragsdaten im Kontext der Online-Antragstellung