Datenschutzmanagementsystem (DSMS)

Verzeichnis von Verarbeitungstätigkeiten der 5G IT Service GmbH

Titel: Übersicht der technischen und organisatorischen Maßnahmen

Historie des Dokuments (Änderungen, Ergänzungen, Revisionen)

Version	Datum	Autor	Kommentar
00	11.08.2018		Ersterstellung in Verbindung mit dem Datenverarbeitungsverzeichnis nach Art. 30, 1
01	20.11.2019		Anpassung nach § 64 BDSG neu
02	02.02.2024		internes Audit

Mitgeltende Unterlagen (Verweise auf weitere Vorgabedokumente, z. B. Anweisungen, Formblätter)

Dokument	Titel	Verantwortung	Aufbewahrungsort	Aufbewahrungsdauer
2.14.1	IT-Sicherheit und Datenschutzkontrollen 04.01.2024	GF	Datenschutzordner	gemäß Auditplan

Anlagen / Hilfsmittel (können unterstützend hinzugezogen werden)

Dokument	Titel
DS-GVO	1. Verordnung (EU)2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
BDSG	6. Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 (BGBl. 1 S. 2097), geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019, BGBl. 1 S. 1626)

Verweise zu internen Managementsystemen, Gesetzen und Normen	
Normen / Gesetze / Vorgaben	Artikel 32 DS-GVO (Sicherheit der Verarbeitung)
Interne Verweise / Datenschutzhandbuch	Datenschutzhandbuch, Kapitel 2.14
Sonstige Verweise	Keine

Inhaltliche Prüfung	Freigabe Unternehmen	Freigabe DSB
Freigabe durch E-Mail fb@fboe.de	Freigabe durch E-Mail 5G IT Service GmbH	Erstellung 02.02.2024

Prozessinformationen	
Bezeichnung	Beschreibung
Prozessart	☐ Managementprozeß (Führungsprozeß) ☐ Operativer Prozeß (Kernprozeß) ☒ Supportprozeß(Unterstützungsprozeß)
Zielsetzung	Zusammenfassung der wesentlichen, vom Unternehmen getroffenen, technischen und organisatorischen Maßnahmen. Diese sollen ein angemessenes Schutzniveau bieten um die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen.
Anwendungsbereich	Unternehmensweit / Unternehmensgruppe
Kennzahlen / Meßgrößen	• getroffene Maßnahmen
Verantwortliche Personen	• Leitung des Unternehmens • IT-Leitung des Unternehmens
Beteiligte Person(en)	• Datenschutzbeauftragter / Datenschutzkoordinator • Informationssicherheitsbeauftragter • Ansprechpartner der Fachbereiche: insbesondere IT und Unternehmenssicherheit
Kontrollierende Person(en)	Datenschutzkoordinator / DSB
Input	• Schutzbedarf • technische Maßnahmen • organisatorische Maßnahmen • Übersicht der Maßnahmen
Output	• Übersicht der Maßnahmen
Kurzbeschreibung	Die Datenschutz-Grundverordnung (DS-GVO) fordert insbesondere in Artikel 32, dass angemessene technische und organisatorische Maßnahmen zu treffen sind, um die Rechte und Freiheiten natürlicher Personen zu schützen, deren Daten das Unternehmen verarbeitet. Dabei muß nicht nur die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos berücksichtigt werden, sondern es sind auch der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen. Das vorliegende Dokument faßt die wesentlichen, seitens des Unternehmens getroffenen, Maßnahmen übersichtlich zusammen. Das Dokument soll dabei als Übersicht dienen und erhebt nicht den Anspruch jede Maßnahme im Detail abzubilden.

Der Gesetzgeber fordert in Artikel 32 DS-GVO zunächst pauschal, dass „angemessene“ technische und organisatorische Maßnahmen getroffen werden. Als konkrete Forderungen wird die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit gefordert. Ferner die rasche Wiederherstellung der Verfügbarkeit der Daten nach einem Zwischenfall. Auch nennt die Verordnung die Pseudonymisierung und Verschlüsselung als geeignete Maßnahmen und fordert regelmäßige Überprüfungen, Bewertungen und Evaluierungen der getroffenen Maßnahmen.

Die Datenschutz-Grundverordnung beschreibt die Anforderungen nur sehr allgemein und überläßt es dem Verantwortlichen die getroffenen Maßnahmen sinnvoll in einer übersichtlichen Struktur abzubilden.

Das deutsche Bundesdatenschutzgesetz, BDSG (nationales Ergänzungsgesetz für Deutschland, geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019, BGB. 1 S. 1626) enthält in § 64 Absatz 3 eine deutlich feinere Gliederung. Auch wenn diese Regelung nur für bestimmte öffentliche Stellen in Deutschland verbindlich ist, kann sie dennoch als sinnvolle Gliederung überall in Europa gesehen werden. Entsprechend ist auch die folgende Darstellung gegliedert.

1. Zugangskontrolle (und Zutrittskontrolle)

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.

- ☒ die Durchführung der Datenverarbeitung erfolgt in:
  - ☒ Büroräumen des Unternehmens
  - ☒ Serverraum / Rechenzentrum des Unternehmens
  - ☒ Externe(s) Rechenzentrum
  - ☒ Cloud-Dienste oder gehostete Software (SaaS)
- ☐ Umzäunung des Firmengeländes
- ☐ Überprüfung der Zutrittsberechtigung zum Firmengelände
- ☐ Wachdienst / Pförtnerdienst
- ☐ Videoüberwachung des Geländes / Außenhaut des Gebäudes
- ☐ Zugänge zum Gebäude sind verschlossen oder während der Öffnungszeiten durch einen Empfang besetzt
- ☒ Absicherung der Fenster und Türen (Sicherheitsglas, Sicherheitsfolie, Gitter oder vergleichbares)
- ☐ Alarmüberwachung des Gebäudes (Bewegungsmelder, Öffnungsmelder, Bruchmelder oder vergleichbares)
- ☐ Bestreifung durch einen Wachdienst außerhalb der Öffnungszeiten des Unternehmens
- ☒ elektronisches Zutrittskontrollsystem
- ☒ Serverraum als eigene Sicherheitszone mit dauerhaftem Verschluss / Zugangskontrolle
- ☒ Videoüberwachung des Serverraumes / Rechenzentrums
- ☒ Anmeldung / Registrierung von Besuchern
- ☒ Abholung von Besuchern durch einen Mitarbeiter
- ☐ weitere Maßnahmen:

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

- ☐ kein Einsatz von Datenträgern außerhalb des IT-Bereiches
- ☐ Sperrung nicht benötigter Schnittstellen, insbesondere USB
- ☒ Verbot des Einsatzes privater Datenträger
- ☒ Verbot des Einsatzes fremder (nicht vom Unternehmen beschaffter) Datenträger
- ☒ Inventarisierung von Datenträgern
- ☐ maschinelle Datenträgerverwaltung (eingebaute Datenträger, Sicherungsmedien, etc.)
- ☐ Alarmierung bei unbefugtem Entfernen von Datenträgern
- ☒ Festlegung von Aufbewahrungsfristen („Lebenszyklus“) von Daten auf Datenträgern
- ☐ sichere Aufbewahrung von Datenträgern (Datensafe, verschlossene Schränke, Transportboxen)
- ☐ Einschränkung der Datenexportrechte in den Anwendungen
- ☐ Überwachung von Datenexporten, u. a. mittels Data Leakage Prevention Tools
- ☒ Arbeitsanweisung zur datenschutzkonformen Löschung von Datenträgern
- ☒ Arbeitsanweisung zur datenschutzkonformen Vernichtung von Datenträgern
- ☐ weitere Maßnahmen:

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

- ☒ Berechtigungskonzept mit revisionsfähiger Zugriffsberechtigungsverwaltung
- ☒ Sperrung des Bildschirms bei längerer Inaktivität des Benutzers
- ☒ Einsatz von Verschlüsselungsalgorithmen
- ☒ Vorgaben für die Dateiorganisation / Ablagestrukturen
- ☒ Protokollierung von Datenzugriffen
- ☒ Trennung von Test- und Produktivsystemen
- ☒ Flächendeckender Einsatz von Virenscannern
- ☒ zentraler Patternserver für Virussignaturen
- ☒ automatisches Reporting über Virenaktivitäten
- ☐ weitere Maßnahmen:

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

- ☒ Festlegung der nutzungsberechtigten Personen
- ☒ Identifikation und Authentifizierung der Benutzer (Benutzername und Kennwort, Biometrie o. ä.)
- ☒ Verschlüsselung von Datenübertragungen
- ☒ Protokollierung der Benutzer und ihrer Aktivitäten
- ☐ weitere Maßnahmen:

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfaßten personenbezogenen Daten Zugang haben.

- ☒ Verhinderung unbefugter externer Zugriffe durch Firewall
- ☒ Berechtigungskonzept mit revisionsfähiger Zugriffsberechtigungsverwaltung
- ☒ Einsatz von Benutzerprofilen, Rollenkonzepten oder vergleichbarem
- ☒ Identifikation und Authentifizierung der Benutzer (Benutzername und Kennwort, Biometrie o. ä.)
- ☒ dedizierte Accounts für administrative Tätigkeiten
- ☐ Einschränkung der Möglichkeiten der direkten Datenbankabfrage („Query“)
- ☒ Protokollierung von Benutzerzugriffen
- ☒ Benutzerbezogene Protokollierung von (Fehl-) Zugriffen
- ☒ Einschränkung der Nutzung von Fernwartungszugängen
- ☐ weitere Maßnahmen:

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

- ☒ Dokumentation der eingesetzten Übertragungs- und Übermittlungsprogramme
- ☒ Protokollierung von Datenübertragungen (Identifikation von Empfängern / Abrufenden)

☒ Festlegung der Übermittlungswege und der zulässigen Datenempfänger
☒ Verschlüsselung der Übermittlungswege (siehe auch Transportkontrolle)
☐ weitere Maßnahmen:

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

☒ Log-Dateien mit Aufzeichnungen zu Datenerfassungen
☒ Log-Dateien mit Aufzeichnungen zu Datenveränderung
☒ Log-Dateien mit Aufzeichnungen zu Datenlöschung
☐ Log-Dateien mit Aufzeichnungen zu Datenübergaben mittels Schnittstellen aus Vorsystemen
☒ es besteht ein restriktives Zugriffsberechtigungskonzept auf die genannten Log-Dateien
☒ Kennzeichnung belegbehafteter Datenerfassungsvorgänge mit dem Kürzel des Sachbearbeiters
☐ weitere Maßnahmen:

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

☒ es erfolgt im Regelfall kein Transport von personenbezogenen Daten auf Datenträgern
☒ sofern personenbezogene Daten auf Datenträgern transportiert werden, erfolgt dies verschlüsselt
☐ alle Datenträgertransporte werden dokumentiert (z. B. Ausgabe- und Rückgabeprotokolle)
☒ der Transport erfolgt in verschlossenen Transportboxen
☒ der Transport erfolgt durch eigene Mitarbeiter oder Mitarbeiter des Auftraggebers
☐ der Transport erfolgt durch Kurierdienste
☒ zum digitalen Datenaustausch kommen folgende Übertragungsarten zum Einsatz:
  ☒ sFTP
  ☒ HTTPs (z. B. Web-Oberflächen, Cloud-Zugriffe)
  ☒ SSL-VPN-Verbindungen, CITRIX oder vergleichbare Standards
  ☐ S/MIME oder PGP Verschlüsselung von E-Mails
  ☒ Sonstiges: DATEV, proprietäre Protokolle im Bereich der Industrierechner, E-Mail
☒ Absicherung des Zugangs zu mobilen Systemen durch Biometrie oder Kennwortschutz
☒ Verschlüsselung der Datenablage auf Notebooks
☐ weitere Maßnahmen:

9. Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

☒ regelmäßige, mindestens tägliche Durchführung einer Datensicherung
☒ Vorhaltung mehrerer Generationen der Datensicherung
☒ gesicherte Aufbewahrung der Datensicherungen:
  ☒ Auslagerung der Backup-Medien an einen gesicherten externen Standort
  ☒ Auslagerung der Backup-Medien in einen anderen Brandschutzabschnitt
  ☐ Lagerung der Backup-Medien in einem Brandschutz-Tresor
  ☒ Durchführung der Datensicherung in einem räumlich getrennten Backup-Rechenzentrum

- ☒ Online-Datensicherung bei einem externen Anbieter
- ☒ Tests zur Wiederherstellbarkeit der Datensicherung
- ☒ es bestehen Wartungs- / Supportverträge mit Dienstleistern
- ☐ dokumentierte Notfallpläne
- ☐ es werden Notfallübungen durchgeführt
- ☐ weitere Maßnahmen:

10. Zuverlässigkeit

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- ☒ regelmäßiges Einspielen von Updates
- ☒ Überwachung des Einspielens von Updates (z. B. zentraler Update-Server, automatisiertes Reporting)
- ☒ führen von Systemlogs, regelmäßige Kontrolle der Logdateien
- ☒ Einsatz eines Monitoring-Systems, automatisierte Alarmierung bei Fehlfunktionen
- ☒ Einsatz redundanter Bauteile (z. B. Netzteile, etc.)
- ☒ Hochverfügbarkeit der Systeme durch
  - ☒ Spiegelung zentraler Systeme
  - ☒ Spiegelung des Rechenzentrums
  - ☐ Sonstiges:
- ☐ weitere Maßnahmen:

11. Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

- ☒ Sensibilisierungsmaßnahmen zur Datenintegrität (z. B. Datenmanipulation, Datenlöschung)
- ☒ restriktive Vergabe von Berechtigungen, insbesondere Änderungs- und Löschrechte
- ☒ Maßnahmen zur Erkennung fehlerhafter Datenübermittlungen
- ☒ Überprüfung der Datenbank auf strukturelle Integrität (Nutzung der Datenbank-Tools)
- ☒ Ermittlung und Kontrolle von Prüfsummen („Checksums“)
- ☒ Erzeugung von Hash-Werten und Zeitstempeln für wichtige Daten
- ☐ digitale Signatur von Dokumenten und Daten
- ☐ Einsatz von Data Integrity Protection (DIP) Lösungen
- ☐ weitere Maßnahmen:

12. Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☒ Verpflichtung der bei der Datenvereinbarung eingesetzten Mitarbeiter zur Wahrung der Vertraulichkeit
- ☒ soweit zutreffend werden Mitarbeiter auf das Fernmeldegeheimnis und Postgeheimnis verpflichtet
- ☒ die Mitarbeiter sind zur Einhaltung einer IT-Benutzerrichtlinie verpflichtet
- ☒ Auftragsverarbeiter werden nur auf Basis eines Vertrages nach Artikel 28 DS-GVO eingesetzt
- ☒ alle in der Datenverarbeitung zum Einsatz kommenden Mitarbeiter erhalten eine Datenschutzunterweisung
- ☐ weitere Maßnahmen:

13. Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:

☒ Maßnahmen zur Wiederherstellbarkeit (siehe Abschnitt „9. Wiederherstellbarkeit“)

☒ Maßnahmen zur Zugangs-, Zutritts- und Zugriffskontrolle (siehe entsprechender Abschnitt)
1. Zugangskontrolle,
5. Zugriffskontrolle (Zutritt),

☒ redundante Stromversorgung durch
- ☒ USV-Anlage für alle relevanten Systeme
- ☒ Stromgenerator zur Überbrückung längerer Stromausfälle
- ☒ redundante Stromzuführung seitens des Versorgers
- ☐ Sonstiges:

☒ redundante Netzanbindung durch
- ☒ mehrere DSL / Standleitungen
- ☐ Backup-Anbindung via Mobilfunk oder Satellit
- ☐ Sonstiges:

☒ Brandschutzmaßnahmen durch
- ☒ Sensoren zur Branderkennung
- ☒ Aufschaltung auf eine Brandmeldeanlage
- ☒ automatisches Löschsystem
- ☒ Feuerschutz des Serverraums (u. a. Brandschutztür, Brandschutzwände)
- ☒ Brandschutz der Kabeldurchführungen im Serverraum
- ☐ Sonstiges:

☒ Redundanz der Datenspeicherung durch
- ☒ Spiegelung der Server / Storagesysteme
- ☒ Spiegelung der Datenträger (z. B. RAID-1)
- ☒ Sicherung der Datenträger durch Paritätsinformationen (z. B. RAID-5/6)

☐ Sonstiges:

weitere Maßnahmen:

14. Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

☒ eigene physische oder virtuelle Umgebung je Mandant
☒ getrennte Mandanten innerhalb der entsprechenden Anwendungen
☒ mandantenbezogenes Berechtigungskonzept zur Verhinderung von Sachbearbeiterzugriffen auf „fremde“ Mandanten
☒ Verpflichtung der Mitarbeiter, Informationen eines Mandanten nicht bei einem anderen zu nutzen
☐ weitere Maßnahmen: