DMS GRUPPE

zuverlässig – innovativ – nachhaltig

Datenschutz- und Datensicherheitskonzept

Stand 20.08.2024
Version 1.8

1 Einleitung

Die vorliegende Übersicht beschreibt den für Auftraggeber der DMS Management Service GmbH (DMS) Stand der Regelungen bezüglich der europäischen Datenschutz-Grundverordnung (EU 2016/679).

Die im Rahmen der Erbringung der Dienstleistungen der DMS zu verarbeitenden personenbezogenen Daten und übriger Geschäftsinterna, stellen einen wesentlich zu schützenden Wert für die DMS dar. Im Besonderen ist deshalb die Sicherheit und Zuverlässigkeit der DMS IT-Systeme, -Dienste und -Anwendungen ebenso wie der vertrauliche Umgang mit personenbezogenen Daten zu gewährleisten. Dazu wurden verschiedene technische und organisatorische Maßnahmen ergriffen, damit die Auftragserfüllung im Einklang mit den gesetzlichen und vertraglichen Anforderungen erfolgt.

2 Regelungen zu den Verantwortlichkeiten im Datenschutz

Datenschutz und Datensicherheit stellen elementare und unternehmensbezogen umzusetzende Anforderungen an den täglichen Geschäftsbetrieb. Hierfür sind die Geschäftsleitung sowie deren maßgebend handelnden Leitungspersonen unmittelbar verantwortlich.

2.1 Geschäftsführung und sonstige verantwortliche Personen

2.1.1 Vertretungsberechtigte Geschäftsführer

Johannes Heibel
Gunther Jahn

2.1.2 Leiter IT

Michael Hopf (Leiter Organisation/IT)

2.1.3 Leiter IT-Service / IT-Administration

Dennis Geitner

2.1.4 Datenschutzbeauftragter

Frank Nitschke

2.1.5 Allgemeine Kontaktdaten

DMS Daten Management Service GmbH
Johannisstraße 5
07545 Gera

Telefon +49 365 55220-0
Fax +49 365 55220-144

www.dms-gruppe.de
info@dms-gruppe.de

2.1.6 Verantwortlichkeiten im Unternehmen

Die verarbeitungsspezifischen Verantwortlichkeiten werden im „Verzeichnis für Verarbeitungstätigkeiten" (nach Art. 30 DSGVO) geführt. Desweiteren haben Projektleiter im Rahmen ihrer allgemeinen Verantwortung die Einhaltung des Datenschutzes im Verantwortungsbereich sicherzustellen.
Beispielhaft sind hier zu nennen:

- Prozesse nach Kapitel 4 einführen & betreiben
- personenbezogene Daten nur im notwendigen Umfang erheben und verarbeiten lassen
- Kontrolle, dass personenbezogene/-beziehbare Daten nur rechtmäßig weitergegeben, eingesehen (technische und organisatorische Absicherungen, insbesondere Zugriffsberechtigungen) und zweckgebunden verarbeitet werden
- Beschäftigten Schulungen zum Umgang mit personenbezogenen/-beziehbaren Daten ermöglichen

Koordiniert werden die Datenschutzmaßnahmen durch den ordentlich bestellten Datenschutzbeauftragten der DMS.

3 Rechtsnormen

Aktuelle relevante Rechtnormen (Gesetzte, Verordnungen, Richtlinien, technische Regeln) erreichen den bestellten Datenschutzbeauftragten über einschlägige Online-Quellen und Verbandsinformationen der GDD e.V. und finden Berücksichtigung.

Relevante Rechtnormen sind u.a.:

- Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG)

4 Beauftragter für Datenschutz

Die Geschäftsleitung hat gemäß Art. 38 ff. DSGVO in Verbindung mit § 38 BDSG einen Datenschutzbeauftragten schriftlich bestellt.

Der Datenschutzbeauftragte wurde auf der Grundlage seiner beruflichen Qualifikation und insbesondere Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 DSGVO genannten Aufgaben.

Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

Grundlage und Maßstab der Aufgabenerfüllung des Datenschutzbeauftragten sind die für die DMS einschlägigen Rechtsvorschriften zum Datenschutz (siehe Ziff. 2). Im Rahmen seiner Aufgabenerfüllung sowie der Anwendung seiner Fachkunde ist der Datenschutzbeauftragte

weisungsfrei. Gegenüber der Geschäftsführung der DMS hat er ein direktes Vortragsrecht und ist dieser unmittelbar unterstellt.

Die festgelegten Aufgaben des Datenschutzbeauftragten umfassen:

- Beratung und Unterrichtung Geschäftsleitung und Beschäftigte hinsichtlich ihrer Pflichten nach der DSGVO und anderer datenschutzrechtlicher Bestimmungen
    - Schulungen
    - Aktualisieren einschlägiger Richtlinien
    - Beratungen bei einer Datenschutz-Folgenabschätzung
    - Zusammenarbeit mit der Aufsichtsbehörde
- Überwachung Einhaltung der DSGVO
    - Verzeichnis Verarbeitungstätigkeiten
    - Prüfungen personenbezogene Datenverarbeitungen
    - gemeinsame Erarbeitung wirksamer Sicherheitskonzepte
    - Berichtswesen
- Bearbeitung Auskunftsersuchen und Anliegen Betroffener
- Ansprechpartner für die Aufsichtsbehörde und ggf. Auftraggeber

5 Einführung personenbezogener Verarbeitungen

Für das datenschutzkonforme Betreiben personenbezogener Verarbeitungen ist der Verarbeitungsverantwortliche zuständig (vgl. Kapitel 2), letztverantwortlich ist die Geschäftsleitung.

Die formale Einführung personenbezogener Verfahren geschieht in Absprache mit dem Datenschutzbeauftragten.
In einem standardisierten Verfahren werden die Grundinformationen über den Prozess an den Datenschutzbeauftragten mitgeteilt. Der Datenschutzbeauftragte prüft den Prozess und gibt eine Stellungnahme ggf. an Geschäftsleitung, IT-Leiter und den Verarbeitungsverantwortlichen. In seiner Stellungnahme können Bedingungen zum Betreiben der Verarbeitung festgelegt werden.

6 Kontrollen

Der Datenschutzbeauftragte überwacht die Einhaltung der DSGVO im Sinne Art. 39 Absatz 1 lit.b DSGVO, insbesondere die ordnungsgemäße Durchführung der Datenverarbeitungen.
Er kontrolliert dazu stichprobenartig ob bestehende Vorgaben in ausreichendem Maße umgesetzt bzw. eingehalten werden.

Über die erforderlichen Maßnahmen und Umsetzungen sind regelmäßig unternehmensinterne Statusberichte zu erstellen.
Diese enthalten:

- die Durchführung einer Bestandsaufnahme zur Feststellung der Erfüllung gesetzlicher Anforderungen
- Ermittlung, Feststellung und Kontrolle des Handlungs- bzw. Änderungsbedarfs in Bezug auf notwendige Schutzmaßnahmen, sowie Festlegung der Zielstellungen
- Entwicklung / Anpassung von (internen) Richtlinien und Arbeitsanweisungen sowie Formularen zur Realisierung der Anforderungen

- Beurteilung / Bewertung der Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen (vgl. Art. 32 DSGVO)
- Überwachungsmaßnahmen der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen
- durchgeführte Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO
- Schulungen und internen Sicherungsmaßnahmen
- Überblick über aufgetretene Problemfelder und deren Bearbeitung.

7 Wahrnehmung Rechte betroffener Personen

Betroffene Personen (Nutzer/Interessenten/Beschäftigte/Anprechpartner) der internetbasierten Datenverarbeitungen können sich mittels der jeweiligen Datenschutzerklärungen oder Merkblätter zum Umfang der Datenverarbeitungen informieren. Die Möglichkeiten der Rechtewahrnehmung hinsichtlich Auskunft, Berichtigung und ggf. Löschung, Widerspruch, Einschränkung, Datenübertragbarkeit sind darin dargelegt. Beschäftigte der DMS werden solchen Ersuchen gemäß den Arbeitsanweisungen nachkommen.
Betroffene dürfen sich zudem vertraulich direkt an den DSB wenden, bspw. über die E-Mail-Adresse datenschutz@dms-gruppe.de.

8 Schulungen und Sensibilisierungen

Der Datenschutzbeauftragte führt mit allen Beschäftigten regelmäßig Schulungen zum Themengebiet Datenschutz und Datensicherheit durch. Die Schulungen erfolgen jährlich, deren Inhalte und Teilnahme wird dokumentiert.

9 Richtlinien zur Sicherstellung von Datensicherheit und Datenschutz

Beschäftigte der DMS Management Service GmbH werden in Richtlinien über die erforderlichen Maßnahmen zur Wahrung von Datensicherheit und Datenschutz sensibilisiert und auf die Einhaltung bestimmter Vorgaben verpflichtet.

Handlungsleitlinien zu Datenschutz und Datensicherheit finden sich in den Dokumenten:

- Verpflichtung auf das Datengeheimnis
- IT-Sicherheitsrichtlinie für Anwender
- IT-Sicherheitsrichtlinie für Systemadministratoren
- Datenschutzleitlinie
- Datenschutz-Richtlinie Datenschutzverletzung
- Datenschutz-Richtlinie Wahrnehmung Betroffenenrechte
- Richtlinie Home-Office
- Richtlinie Informationsklassifizierung

10 getroffene technische und organisatorische Schutzmaßnahmen

Allgemeine Strukturen und Vorgehensweisen zum organisatorischen Schutz von personenbezogenen Daten sind in vorgenannten Richtlinien fixiert.

Es werden prinzipiell alle Beschäftigte auf die Einhaltung des Datengeheimnisses schriftlich verpflichtet.
Zudem greifen abteilungs- und standortübergreifend standardisierte Starter-Changer-Leaver-Prozesse.
Darüberhinaus sind technische und organisatorische Schutzmaßnahmen festgehalten im:

- Notfallplan/BCM hinsichtlich Verfügbarkeit
- Verzeichniseintrag jeweiliger Verarbeitungen

Es wurden die im Folgenden dargestellten organisatorischen und technischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten vor unbefugter Kenntnisnahme (Vertraulichkeit), Verfälschung (Integrität) und Verlust (Verfügbarkeit) gemäß Art. 32 DSGVO ergriffen.

Die Schutzmaßnahmen gelten für jegliche personenbezogene Datenverarbeitungen im Sinne des Art. 4 Satz 1 Nr.2 DSGVO soweit diese räumlich und technisch von DMS-Beschäftigten durchgeführt werden.

Schutzziel (DSGVO)	Zutritts-kontrolle	Zugangs-kontrolle	Zugriffs-kontrolle	Weitergabe-kontrolle	Eingabe-kontrolle	Auftrags-kontrolle	Verfügbarkeits kontrolle	Getrennte Verarbeitung
Vertraulichkeit	X	X	X	X		X		X
Integrität				X	X	X		X
Verfügbarkeit						X	X	

10.1 Zutrittskontrolle

Ziel: Unbefugten den räumlichen Zutritt zu DV-Anlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Die folgenden Angaben gelten für die Geschäftsräume der DMS Management Service GmbH in dessen Standorten.

10.1.1 Objektsicherung Geschäftsräume

- Besucher, Fremdbeschäftigte und Dritte müssen sich anmelden (klingeln)
- der Zutritt unternehmensfremder Personen außerhalb der Geschäftszeiten ist unterbunden

- weitere Maßnahmen sind
    - Schließanlage

  - Ausweistragepflicht für Beschäftigte
  - Ausweistragepflicht für Besucher
  - Besucherbuch

- Zutritt ausschließlich über personengebundene Token oder Schlüssel
  - formalisierte Tokenausgabe (mit Anweisung)
  - Schlüsselausgabe wird protokolliert für die DMS-Räumlichkeiten (Schlüsselbuch)
  - formelle Regelung mit einzuleitenden Folgemaßnahmen bei Verlust des Eintritts-Chips

10.1.2 Sicherheitszonen

- die Geschäftsräume auf der Etage sind durch ein Zutrittskontrollsystem (Token) zutrittsgesichert

- Besucherregelungen sind in der IT-Sicherheitssicherheitsrichtlinie festgehalten (Abholung/Begleitung durch zuständige Beschäftigte)

- das Reinigungspersonal hat nur Zutritt zu den Räumen, wenn Beschäftigte am Arbeitsplatz sind.
  Es besitzt keine Schlüssel zu den Räumen der DMS.

- weitere Sicherheitszonen
  - closed-shop Geschäftsräume
  - Serverräume
  - Personalabteilung
  - Archiv

- Datenträger (Arbeitsplatzrechner, sowie Server) befinden sich außerhalb der Geschäftszeiten in abgeschlossenen Räumen oder sind verschlüsselt

10.2 Zugangskontrolle

Ziel: Unbefugten die Nutzung der IT-Systeme, mit denen personenbezogene Daten verarbeitet werden, verwehren.

10.2.1 Unterbindung unbefugte Nutzung IT-Systeme in Geschäftsräumen

- Abfrage Benutzerkennung mit Passwortschutz und automatische Kontrolle Passwortkonvention
  - Zeichenmindestlänge 8
  - Passwortkomplexität verbietet Trivialkennworte, fordert Groß/Kleinschreibung, Zahl sowie Sonderzeichen
  - Passworthistorie von 6 Generationen

- nach 5 fehlgeschlagenen Authentifizierungsversuchen erfolgt Account-Sperrung, Entsperrung ist bei IT zu beantragen

- Bildschirmsperre mit Passwortaktivierung bei Verlassen des Arbeitsplatzes
- Endpointsecurity auf allen Clients
- separierende VLAN
- mehrheitliche Arbeit auf Terminalservern, Sitzungsaufnahme wird durch IT-Abteilung und ggf. Auftraggebern freigegeben
- Aufbewahrung Sicherungsdatenträger in Tresor (anderer Brandabschnitt) mit entspr. kleinen Kreis an Zugangsberechtigten
- Firewallbetreuung erfolgt durch einen Sicherheitsdienstleister
- IDS

10.3 Zugriffskontrolle

Ziel: Die unerlaubte Tätigkeit in IT-Systemen außerhalb eingeräumter Berechtigungen zu verhindern.

10.3.1 Berechtigungskonzepte allgemein

- systemseitig und anwendungsseitig erfolgt eine Authentifizierung von Diensten und Nutzern entsprechend den Berechtigungskonzepten
- differenzierte Berechtigungen für Daten, Anwendungen und Betriebssysteme (z.B. Lesen, Löschen, Ändern)
- Trennung von Berechtigungsvergabe und Berechtigungsbewilligung
- Dokumentation Berechtigungsantrag und -vergabe in Ticketsystem
- wenn auf Auftraggebersystemen gearbeitet werden die vorgegebenen Rollen/Berechtigungskonzepte beachtet
- jeder Nutzer muß sich wahrheitsgemäß am System authentisieren, die Weitergabe der Zugangsdaten ist verboten

10.3.2 Berechtigungskonzepte Verwaltungsoberfläche DMS PMT (falls eingesetzt)

- Falls ein Zugriff von Beschäftigten des Auftraggebers auf DMS PMT vorgesehen ist, erfolgt dieser rollenbasiert
- Rollen werden in einem Berechtigungsmanager konzeptioniert mit Beschränkung auf ein Minimum an zur Aufgabenerfüllung erforderlicher Rechte (Least-Privileges-Konzept)

10.3.3 Protokollierung

- Nachweis des administrativen Zugriffs auf IT-Systeme durch Vorgangsprotokolle
- anwendungsseitig erfolgt benutzerscharfe Protokollierung der Aktivitäten, wie Erstellen, Änderungen und Löschungen von Datensätzen mit Zeitstempel

10.3.4 Datenträger

- Sicherstellung das Datenträger mit personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
    - hierzu existieren Maßnahmen und Regelungen bezüglich der berechtigten Personen, der Aufbewahrung, der Ausgabe und der Vernichtung von Daten und Datenträgern
- es bestehen Regelung zur Datenträgeraufbewahrung unter Berücksichtigung der Aufbewahrungsfristen und der eindeutigen Kennzeichnung von Datenträgern in Archivräumen, Tresoren und Schränken
- eine Regelung besteht zur datenschutzgerechten Vernichtung von Datenträgern unter Berücksichtigung der Aufbewahrungsfristen und der eindeutigen Kennzeichnung von Datenträgern usw.
- es sind Datenschutztonnen aufgestellt, die der sachgerechten Vernichtung zugeführt werden durch einen zertifizierten Dienstleister
- die Wiederherstellung von Daten aus Backups (Wer kann und darf Wann, auf wessen Anforderung Backup-Daten einspielen?) ist verbindlich geregelt
- Einbringen privater Datenträger in IT-Systeme nicht gestattet und Datenträger werden von Firewall/Endpointsecurity geprüft

10.4 Weitergabekontrolle

Ziel: Die Weitergabe personenbezogener Daten (elektronische Übertragungen, Datentransport, Übermittlungskontrollen) zu sichern.

10.4.1 generelle Festlegungen Datentransport

- es finden im Rahmen der Auftragserfüllung einzig Zugriffe auf Auftraggebersysteme statt. Datenträgertransporte sind nicht geplant

10.4.2 generelle Maßnahmen Datenübermittlung

- alle zwischen Standorten und Auftraggebern übertragenen Daten werden verschlüsselt übertragen (VPN)

- Verbindung Befugter zu Servern ist ausschließlich einem engen festgelegten Personenkreis möglich
- Einsatz zertifizierter Netzwerk-Hardware
- Wartung sensibler Hardware durch zertifiziertes Personal

10.5 Eingabekontrolle

Ziel: Die Prüfbarkeit der eingegebenen, veränderten und entfernten Daten.

10.5.1 Umfang Protokollierung

- Benutzerberechtigungen sind differenziert und beschränkt auf den zur Aufgabenerfüllung notwendigen Umfang
- es erfolgt systemseitig eine automatisierte Protokollierung Serverzugriffe bzw. administrativer Nutzer- und Diensteaktivitäten
- Protokollierung Administratortätigkeiten als Standardeinstellung des jeweiligen Servers

10.5.2 Aufbewahrungsfristen Protokolle

- darüberhinaus erfolgt die Löschung anwendungsspezifischer Protokolle auf Auftraggeberwunsch
- die Log-Rotation-Settings der jeweiligen Logarchive orientieren sich an dienste- und anwendungsspezifischen Erfordernissen und können in Absprache mit dem Auftraggeber geändert werden

10.6 Auftragskontrolle

Ziel: Gewährleistung einer weisungsgemäßen Auftragsdatenverarbeitung.

- Verpflichtung Beschäftigte Auftragnehmer auf das Datengeheimnis erfolgte
- regelmäßige Schulungen Beschäftigte Auftragnehmer sowie in jedem Fall bei Einstellung
- Bestellung Datenschutzbeauftragter bei Auftragnehmer
- gültige Auftragsdatenverarbeitungsverträge mit Auftragnehmer (Subunternehmen) liegen vor
- Auftragnehmer (Subunternehmen) wies vergleichbare oder höhere Datenschutzstandards in den technischen und organisatorischen Schutzmaßnahmen nach

- alle Auftragsverarbeitungen (Subunternehmen) bedürfen prinzipiell einer schriftlich geprüften Datenschutz-Vereinbarung nach Art. 28 DSGVO mit dem Auftraggeber

- alle Vertragsbestandteile von Auftragsverarbeitungen erfüllen die Anforderungen aus Art. 28 DSGVO

- Protokollierung und Prüfung der Fernwartungstätigkeit (Firewalladministration, Wartung und Pflege der Firewall) durch Beschäftigte IT

- Unterauftragnehmer (Subunternehmen) haben typischerweise keinen Zugriff auf Daten der Auftraggeber

10.7 Verfügbarkeitskontrolle

Ziel: Gewährleistung das personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

10.7.1 Monitoring

- verschiedene Statusmeldungen kritischer Dienste zur Aufrechterhaltung der Betriebsbereitschaft (Monitoring) werden protokolliert, Abweichungen von Soll-Zuständen werden bewarnt

10.7.2 Backups

- auftragsbezogene Backups obliegen dem Auftraggeber (Arbeiten erfolgen auf Systemen des Auftraggebers)

- falls seitens DMS Backups erfolgen, werden diese automatisch 1*tgl. durchgeführt, deren Aufbewahrungsdauer erfolgt in Absprache mit Auftraggebern

    - Übermittlung und Speicherung zu/auf Backup-Server erfolgt verschlüsselt

    - es erfolgt eine Versionierung der Vollsicherungen

    - katastrophensichere Aufbewahrung von Produktiv- und Backupsystemen in getrennten Rechenzentren

10.7.3 Notfall- und Wiederanlaufverfahren

- erprobter Notfallmaßnahmenplan im Katastrophenfall mit klaren Verantwortlichkeiten und Vertreterregelungen

- DMS verfügt über eine Archivordnung der Backups

- Regelungen für Sicherungen, Duplikatserstellung, Auslagerung und Rekonstruktion von Datenbeständen bestehen

10.7.4 weitere Maßnahmen Verfügbarkeit

- Brandmelder im Geschäftsbereich
- Anlagen Brandfrüherkennung in Räumen DV-Anlagen
- automatische Aufschaltung Feuerwehr
- verschiedene Brandabschnitte innerhalb der Etage
- ausreichend dimensionierte USV (Geschäftsbereich und DV-Anlagen)
- Raid 0,1,5,6 (Serverseitig)
- redundante Company Call-Internetanbindungen
- organisatorische Redundanz durch mgl. Rückgriff auf andere Standorte

10.8 Trennungsgebot

Ziel: Gewährleistung das zu unterschiedlichen Zwecken erhobene Daten unterschiedlich verarbeitet werden.

- Testserver sind getrennt von Produktivservern, es werden keine personenbezogene Auftraggeberdaten zu Testzwecken verwendet
- Kundendaten werden logisch getrennt verarbeitet durch die Virtualisierungsstrategie und VLAN-Separierung

10.9 Datenschutz per Design und als Voreinstellung

Ziel: Vorgaben datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung (Art. 25 Abs. 2 DS-GVO) umsetzen.

- Verschlüsselungen von Daten im Transfer und in Speichern wo indiziert
- Pseudonymisierung von Daten soweit dies im Verantwortungsbereich der DMS liegt und prozessseitig möglich ist

10.10 regelmäßige Evaluierung der Schutzmaßnahmen

Ziel: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit Datenverarbeitung auf Dauer sicherzustellen (Art. 32 Abs. 1 DS-GVO)

- Datenschutz-Management mit regelmäßigen Prüfungen Angemessenheit Datenschutzorganisation

- Incident-Response-Management (strukturierte Prozesse mit Arbeitsanweisungen)