BMS Corporate Solutions GmbH

Technische und Organisatorische Maßnahmen
nach Art. 32 DS-GVO

Düsseldorf, 21.08.2025

BMS Corporate Solutions GmbH
Fürstenwall 172,
40217 Düsseldorf

Telefon: (0211) 302127-00
Telefax: (0211) 302127-09
www.bms-cs.de | info@bms-cs.de

Geschäftsführung:
Michael Luks
Dr. Klaus Segbers

Amtsgericht Düsseldorf HRB 90481
USt-ID-Nr.: DE 332846069
Gläubiger ID Nr.: DE 30 ZZZ 0000
2334 898

Volksbank Westmünsterland eG
IBAN: DE05 4286 1387 0388 5473 00
BIC: GENODEM1BOB

Volksbank Krefeld eG
IBAN: DE22 3206 0362 4039 3320 06
BIC: GENODED1HTK

Inhalt

Zweck des Dokuments 3
Technische und organisatorische Maßnahmen 4
Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 4
Zutrittskontrolle 4
Zugangskontrolle 4
Zugriffskontrolle 5
Trennungskontrolle 6
Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) 6
Integrität (Art. 32 Abs. 1 lit. b DS-GVO) 6
Weitergabekontrolle 6
Eingabekontrolle 7
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO) 7
Verfügbarkeitskontrolle 7
Wiederherstellbarkeit 8
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO) 8
Datenschutzmanagement 8
Datenschutzfreundliche Voreinstellung (Art. 25 DS-GVO) 8
Kontrolle der Unterauftragnehmer 8
Regelmäßige Kontrollen, Dokumentation und Optimierung 9
Incident-Response-Management 9

Zweck des Dokuments

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen der DS-GVO erfüllt werden.

Zudem fordern die Datenschutzgesetze des Bundes und der Länder, dass für jede Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen auszuwählen und umzusetzen sind, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind.

In den folgenden Abschnitten werden die technischen und organisatorische Maßnahmen nach Artikel 32 der Datenschutz-Grundverordnung (DS-GVO) der BMS Corporate Solutions GmbH beschrieben.

Technische und organisatorische Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren:

- Klingelanlage
- Empfang / Rezeption
- Einbruchshemmende Türen
- Umschlossene Betriebsräume
- Alarmgesicherte Betriebsräume
- Führung eines Verzeichnisses von Zutrittsmedien
- Verwendung von Sicherheitsschlüsseln und Transpondern
- Schlüsselvergabe nur an berechtigte Personen (Schlüsselregelung)
- Protokollierung von Besuchern, Begleitung durch eigene Mitarbeiter
- Keine Einsicht auf Bildschirme von außerhalb des Gebäudes möglich
- Sorgfältige Auswahl von Reinigungspersonal und externen Dienstleistern
- Zutritt zu Serverräume ist auf ausgewählte IT-Administratoren beschränkt
- Schaffung von verschiedenen Sicherheitszonen (z. B. gemeinsam genutzte Bereiche, sensible Bereiche, IT-Infrastruktur)

Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Einsatz von VPN bei Remote-Zugriffen
- Automatische Sperrung des Bildschirms
- Verpflichtung des Personals auf Vertraulichkeit
- Daten werden verschlüsselt in externen Backup-Systemen gelagert
- Verschlüsselung von mobilen Datenträgern, Mobilgeräten und Notebooks
- Schulungen zum Umgang mit Authentifizierungsverfahren und -mechanismen
- Remote-Zugänge durch verschlüsselte VPN-Tunnel mit zentraler Anmeldung
- Absicherung der DV-Systeme und Netzwerke gegen Zugänge von außen mittels Firewall
- Zugang zu Computern nur mit Hilfe gesicherter Authentifizierungsverfahren (Benutzerkonto/Passwort)
- Keine Mehrfachverwendung eines Passworts für verschiedene Dienste, sofern kein zentrales Identitätsmanagement verwendet wird

- Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT muss eine Passwortänderung durch den Nutzer erfolgen
- Geregelte Prozesse zur zentralen Verwaltung von Benutzeridentitäten, sowie Rechtevergabe/-entzug bei Eintritt, Veränderung und Austritt von Mitarbeitern auf Grundlage von Berechtigungskonzepten

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Intrusion Detection
- SIEM-Überwachung
- Multi-Faktor-Authentifizierung
- Bereitstellung von Blickschutzfolien
- Minimale Anzahl an Administratoren
- Rollenbasierte Berechtigungskonzepte
- Löschungsprotokolle und Löschkonzepte
- Konzept zur Laufwerksnutzung und –Zuordnung
- Kontosperrungen nach mehreren Fehlversuchen
- Prüfung von Zugriffen auf Anwendungen und Dateien
- Stichprobenartige Auswertung von Zugriffsprotokollen
- Regelmäßige Überprüfung der Zugriffsberechtigungen
- Einsatz von Berechtigungskonzepten nach Need-to-know-Prinzip
- Erzwungene Passwortlänge und -komplexität gemäß Passwortrichtlinie
- Trennung der Netzwerke in USER-Netze und Admin-Netze (getrennte VLANs)
- Trennung der Berechtigungsbewilligung (organisatorisch) und Vergabe (technisch)
- Erteilung und Nutzung von Administratorenrechten auf das Notwendigste begrenzt
- Datenschutzkonforme Vernichtung von Datenträgern und vertraulichen Unterlagen
- Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen
- Passwörter werden nach einem Sicherheitsvorfall gesperrt und müssen vom Nutzer neu vergeben werden (risikoorientierte Passwortänderungen)

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Festlegung von Datenbankrechten
- Separierung von Dateien bei Datenbanken
- Datensätze sind mit Zweckattributen versehen
- Trennung von Speicherbereichen nach Mandanten
- Physische bzw. logische Trennung von Datenbeständen
- Datensätze werden nach Vertraulichkeit klassifiziert
- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Trennung von Zugriffen auf Basis von Organisations-/Abteilungs-/Teamgrenzen

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahmen, die gewährleisten, dass bei der Verarbeitung personenbezogener Daten in einer Weise, die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

- Weitergabe von Daten nur in anonymisierter oder pseudonymisierter Form, falls möglich
- Verwendung von Pseudonymisierungs- und Anonymisierungsverfahren sofern verfahrenstechnisch sinnvoll. In diesen Fällen erfolgt die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- E-Mail-Versand mit Verschlüsselung
- Einsatz von zentral verwalteten E-Mail-Signaturen
- Verschlüsselung aller Daten „in transit“, „at rest“ und „in use“
- Bereitstellung über verschlüsselte Verbindungen wie sftp oder https

- Kein unverschlüsselter Versand personenbezogener Daten per E-Mail
- Sorgfältige Auswahl von Transportpersonal/-fahrzeugen bzw. sichere Verpackungen
- Einsatz der Systeme nur im privaten Netzwerk oder über verschlüsselte Verbindungen in öffentlichen Netzwerken
- „Data Loss Prevention“-Mechanismen zur Identifikation personenbezogener Datensätze und Verhinderung von Datenweitergaben (E-Mails, Downloads, Dokumente)

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Kontrolle der Dateneingabe
- Protokollierung und Auswertung von Systemprotokollen
- Protokollierung von Eingaben, Änderungen und Löschungen
- Organisatorische Festlegung der Zuständigkeiten für die Eingabe
- Protokollauswertung und Sicherung mehrerer Versionssätze im Rahmen von Backups
- Veränderung/Löschungen von personenbezogenen Daten durch den Auftragnehmer erfolgen ausschließlich nach Beauftragung durch den Auftraggeber

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Einsatz von Feuerlöschern
- Backup- und Recovery-Konzept
- Regelmäßige Produkt-/Software-Updates
- Getrennte Aufbewahrung der Sicherungen
- Einsatz von Feuer- und Rauchmeldeanlagen
- Einsatz von Firewalls, Virenscannern und Spam-Filtern
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Notfallkonzept und Notfallplan (Business Continuity Management)
- Regelmäßige Untersuchung von Hard- und Software-Schwachstellen
- Nutzung von Systemen zum Schutz vor Blitzschäden und Spannungsschwankungen
- Einsatz von unterbrechungsfreien Stromversorgungen (USV) an zentralen Komponenten
- Klimatisierung und Überwachung von Temperatur und Feuchtigkeit an zentralen Systemen

Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

- Spiegelung von Festplatten und Systemen
- Redundante Sicherung von Daten und Systemen
- Vertretungsregelungen für abwesende Mitarbeiter
- Auslagerung von verschlüsselten Sicherungskopien
- Regelmäßige Überprüfung der Wiederherstellbarkeit

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)

Datenschutzmanagement

- Benennung eines Datenschutzbeauftragten
- Softwarelösungen für Datenschutzmanagement im Einsatz
- Durchführung interner Audits zum Datenschutzmanagement
- Informationspflichten nach Art. 13 und 14 DS-GVO werden erfüllt
- Schulung von Personal zu Datenschutz und Informationssicherheit
- Durchführung einer Datenschutz-Folgenabschätzung (nach Bedarf)
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen (Datenschutzhandbuch)

Datenschutzfreundliche Voreinstellung (Art. 25 DS-GVO)

- Einfache Ausübung des Widerrufsrechts
- Berücksichtigung der Datenschutzgrundsätze bei der Verarbeitung
- Es werden nicht mehr personenbezogene Daten erhoben als erforderlich
- Regelmäßige Sensibilisierung (Infoveranstaltungen, Newsletter, Schulungen)
- Verarbeitung personenbezogener Daten nur für festgelegten Verarbeitungszweck

Kontrolle der Unterauftragnehmer

- Abschluss von Verträgen zur Auftragsverarbeitung
- Regelmäßige Überprüfung auf Eignung der Dienstleister
- Zentrale Erfassung vorhandener Dienstleister (Zentrales Auslagerungsmanagement)

- Schriftliche Weisungen und Festlegung der Zuständigkeiten, Kontrollrechte vereinbart
- Sichtung vorhandener IT-Sicherheitszertifikate und laufende Kontrolle der Auftragnehmer
- Sorgfältige Auswahl geeigneter Dienstleister aufgrund von Standort und Datenschutz-Maßnahmen (Vorabüberzeugungspflicht)

Regelmäßige Kontrollen, Dokumentation und Optimierung

- Zertifiziertes Internes Kontrollsystem nach IDW PS 951
- Durchführung von Audits im Rahmen der Informationssicherheit
- Regelmäßige interne Kontrolle der getroffenen Sicherungsmaßnahmen
- Prüfungen des Datenschutzbeauftragten auf Einhaltung der Prozesse und Vorgaben
- Hinweisgebersystem zur Meldung von illegalem, unethischem, missbräuchlichem Verhalten
- Regelmäßige Kontrollen der Verarbeitungsverfahren; Maßnahmen basieren auf Stand der Technik und Schutzbedürftigkeit

Incident-Response-Management

- Einberufung eines Notfallgremiums bei Sicherheitsvorfällen
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Dokumentation von Sicherheitsvorfällen und Verletzungen des Schutzes personenbezogener Daten
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten