BMS Corporate Solutions GmbH

technische und organisatorische Maßnahmen
nach Art. 32 DS-GVO

Düsseldorf, 20.09.2023

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:
Markus Kons
Michael Luks
Dr. Klaus Segbers

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

Volksbank Düsseldorf Neuss eG
IBAN: DE 03 3016 0213 0056 229 019
BIC: GENODED1DNE

Inhalt

1. Zweck des Dokumentes

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.

2. Technische und organisatorische Maßnahmen

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

2.1.1. Zutrittskontrolle (Räume und Gebäude)

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 Schlüsselverzeichnisses
- Verwendung von Sicherheitsschlüsseln und Transpondern
- Schlüsselvergabe nur an berechtigte Personen (Schlüsselregelung)
- Protokollierung von Besuchern, Begleitung durch eigene Mitarbeiter
- Sorgfältige Auswahl von Reinigungspersonal und externen Dienstleistern

2.1.2. Zugangskontrolle

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

- Intrusion Detection
- SIEM-Überwachung
- Erzwungene Passwort-Richtlinien
- Einsatz von VPN bei Remote-Zugriffen
- Verschlüsselung aller Daten „In Transit“
- Automatische Sperrung des Bildschirms
- Mehr-Faktor-Authentifizierung falls möglich
- Verpflichtung des Personals auf Vertraulichkeit
- Kontosperrungen nach mehreren Fehlversuchen
- Protokollierung und Auswertung von Systemprotokollen
- Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- Daten werden verschlüsselt in externen Backup-Systemen gelagert
- Einsatz stets aktuell gehaltener Anti-Viren-Software (Server und Clients)
- Zutritt zu Serverräume ist auf ausgewählte IT-Administratoren beschränkt
- Verschlüsselung von mobilen Datenträgern, Mobilgeräten und Notebooks
- Remote-Zugänge durch verschlüsselte VPN-Tunnel mit zentraler Anmeldung
- Trennung der Netzwerke in USER-Netze und Admin-Netze (getrennte VLANs)
- Absicherung der DV-Systeme und Netzwerke gegen Zugänge von außen mittels Firewall

- Prozesse für Rechtevergabe/-entzug bei Eintritt, Veränderung und Austritt von Mitarbeitern
- Zugang zu Computern nur mit Hilfe gesicherter Authentifizierungsverfahren (Benutzerkonto/Passwort)

2.1.3. Zugriffskontrolle (auf Daten und Informationen)

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:

- Löschungsprotokolle
- Minimale Anzahl an Administratoren
- Rollenbasierte Berechtigungskonzepte
- Mehr-Faktor-Authentifizierung falls möglich
- Konzept zur Laufwerksnutzung und –Zuordnung
- Regelmäßige Überprüfung der Zugriffsberechtigung
- Stichprobenartige Auswertung von Zugriffsprotokollen
- Protokollierung von Zugriffen auf Anwendungen und Dateien
- Einsatz von Berechtigungskonzepten nach Need-to-know-Prinzip
- Admin-Accounts nur mit Multi-Faktor-Authentifizierung (MFA-Verfahren)
- Trennung der Berechtigungsbewilligung (organisatorisch) und Vergabe (technisch)
- Erteilung und Nutzung von Administratorenrechten auf das Notwendigste begrenzt
- Datenschutzkonforme Vernichtung von Datenträgern und vertraulichen Unterlagen

2.1.4. 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
- Trennung von Entwicklungs-, Test- und Produktivsystemen
- Trennung von Zugriffen auf Basis von Organisations-/Abteilungs-/Teamgrenzen

2.1.5. Pseudonymisierung (Artikel 32 Abs. 1 lit. a DS-GVO; Artikel 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.

- 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
- Weitergabe von Daten nur in anonymisierter oder pseudonymisierter Form

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

2.2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger 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:

- Einsatz von E-Mail-Signaturen
- E-Mail-Versand mit Verschlüsselung
- Keine Einsicht auf Bildschirme von außerhalb des Gebäudes möglich
- Bereitstellung über verschlüsselte Verbindungen wie sftp oder https
- E-Mail-Richtlinie bzw. 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 (IPsec verschlüsselter VPN-Tunnel)
- „Data Loss Prevention“-Mechanismen zur Identifikation personenbezogener Datensätze und Verhinderung von Datenweitergaben (E-Mails, Downloads, Dokumente)

2.2.2. 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 von Eingaben, Änderungen und Löschungen
- Organisatorische Festlegung der Zuständigkeiten für die Eingabe
- Protokollauswertung und Sicherung mehrere Versionssätze im Rahmen des Backups
- Veränderungen/Löschungen von personenbezogenen Daten durch den Auftragnehmer erfolgen ausschließlich nach Beauftragung durch den Auftraggeber

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

2.3.1. Verfügbarkeitskontrolle

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

- Einsatz von Feuerlöschern
- Notfallkonzept und Notfallplan
- 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
- 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

2.3.2. 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

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

Datenschutzmanagement

- Softwarelösungen für Datenschutzmanagement im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Personal (nach Bedarf)
- Benennung eines Datenschutzbeauftragten
- Durchführung einer Datenschutz-Folgenabschätzung (nach Bedarf)
- Informationspflichten nach Art. 13 und 14 DS-GVO wird nachgekommen

Datenschutzfreundliche Voreinstellung (Art. 25 DS-GVO)

- Einfache Ausübung des Widerrufsrechts des Betroffenen
- Verarbeitung personenbezogener Daten nur für den festgelegten Verarbeitungszweck
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Berücksichtigung der Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten
- Regelmäßige Sensibilisierung (Infoveranstaltungen, Newsletter, Schulungen) der Mitarbeiter für das Thema Datenschutz

Kontrolle der Unterauftragnehmer

- Zentrale Erfassung vorhandener Dienstleister
- Regelmäßige Überprüfung auf Eignung der Dienstleister
- Abschluss von Verträgen zur Auftragsverarbeitung
- 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

- Es finden regelmäßige Kontrollen der Verarbeitungsverfahren statt. Basierend auf dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten, werden entsprechende Maßnahmen ergriffen, um den Datenschutzgrundsätzen gerecht zu werden
- Regelmäßige interne Kontrolle der getroffenen Sicherungsmaßnahmen. (ggf. Anpassung an den Stand der Technik)
- Prüfungen des Datenschutzbeauftragten auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme

Incident-Response-Management

- 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