Technische und organisatorische Maßnahmen (TOM) zum Datenschutzkonzept i.S.d Art. 32 DSGVO

Version letzte Freigabe
Gültig ab: letzter Freigabe

OPTIMAL SYSTEMS GmbH
Unternehmenszentrale
Cicerostraße 26
10709 Berlin

Änderungsübersicht und Freigabeinformationen

Vers	Erstellt durch	Änderung	Erstellt am	Freigabe durch	Freigabe am
2.0.0	Stefan Eberle	Review, Strukturanpassung; Änderungsübersicht neues Format (ab 2.0.0 Einträge)	01.04.20209	Gregor Wolf	06.04.2020
3.0.0	Stefan Eberle/Jasin Hahne/Lisa Gough	Korrektur von Verweisen und kleinen Fehlern und Datumsangaben sowie Überarbeitung von 3 Pseudonymisierung; Änderung durch die Colt Colocation; Wegfall von AppWhitelisting	19.06.2020	Gregor Wolf	01.07.2020

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Inhaltsverzeichnis

1	**Einleitung**	**4**
2	**Maßnahmen zur Gewährleistung der Vertraulichkeit**	**5**
2.1	Zutrittskontrolle	5
2.2	Zugangskontrolle	5
2.3	Zugriffskontrolle	6
2.4	Auftragskontrolle	6
2.5	Trennungskontrolle	7
3	**Pseudonymisierung und Verschlüsselung**	**8**
4	**Maßnahmen zur Gewährleistung der Integrität**	**8**
4.1	Weitergabekontrolle	8
4.2	Eingabekontrolle	8
5	**Verfügbarkeit und Belastbarkeit**	**9**
5.1	Verfügbarkeitskontrolle	9
5.2	Wiederherstellbarkeit	10
6	**Regelmäßige Überprüfung, Bewertung und Evaluierung**	**11**

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

1 Einleitung

In diesem Dokument werden die im Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit“, Version 7.0 – Abschnitt 5.2 angeführten Maßnahmen dargelegt.

Der Artikel 32 der Datenschutzgrundverordnung (DS-GVO) – Sicherheit der Verarbeitung – benennt einzelne technische und organisatorische Maßnahmen konkret bzw. kategorisiert diese anhand ihrer Schutzziele. Im vorliegenden Dokument werden sowohl die explizit benannten Maßnahmen als auch die Maßnahmen, die sich in der Praxis bewährt haben - und als Stand der Technik zu bezeichnen sind - den jeweiligen Schutzzielen zugeordnet.

Soweit sich für öffentliche Auftraggeber besonderer Anforderung aus dem Teil 3 des Bundesdatenschutzgesetzes (BDSG) ergeben, werden diese als erweiterte Anforderungen im Sinne des Kapitel 4.3 des Datenschutzkonzepts angesehen und auftragsbezogen separat dokumentiert.

Die hier aufgelisteten Maßnahmen unterliegen sich ändernden technischen Voraussetzungen und Anforderungen, sowie Bedrohungs-Szenarien und werden dementsprechend fortlaufend angepasst. Diese Änderungen werden regelmäßig in das vorliegende Dokument übernommen.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

2 Maßnahmen zur Gewährleistung der Vertraulichkeit

2.1 Zutrittskontrolle

In diesem Abschnitt werden Maßnahmen benannt, die einen räumlichen Zutritt Unbefugter verhindern.

- Zutritt ist durch ein Berechtigungskonzept geregelt
- Zutritt wird über elektronische Berechtigungsausweise bzw. Schlüssel beschränkt und überwacht
- Zutritt von Besuchern wird durch eigene Mitarbeiter begleitet
- Außerhalb der Arbeitszeit werden die Räumlichkeiten durch eine Alarmanlage überwacht
- Gemäß Schutzbedarf existieren abgestufte Sicherheitsbereiche mit kontrolliertem Zutritt
- Die produktionsrelevanten, datenhaltenden Server sind in ein professionelles ISO 27001/ISO 14001/ISO 9001 zertifiziertes Tier-3 Rechenzentrum ausgelagert
    - Zutritt zum Rechenzentrum nur für berechtigte Personen
    - PIN Schutz der dedizierten Racks
    - 24x7 Wachschutz, sowie Videoüberwachung
- Wartungsarbeiten an Systemen der Datenverarbeitung grundsätzlich nur unter Aufsicht

2.2 Zugangskontrolle

Die Zugangskontrolle umfasst die Maßnahme zur Verhinderung eines unbefugten Eindringens in bzw. einer unbefugten Nutzung von Datenverarbeitungsanlagen.

- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Prozess zum Rechteentzug bei Funktionswechsel von Mitarbeitern
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- Verwendung von personalisierten Benutzerkennungen / Passwörtern
    - Die zu verwendenden Passwörter unterliegen technisch erzwungenen Richtlinien hinsichtlich Komplexität, Änderungsintervallen, Passwortrotation und automatischer Sperrung bei Falscheingabe des Passwortes
    - Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
    - Passwörter werden als Hash-Werte gespeichert

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

- Zentraler und dezentraler Virenschutz an allen der Datenverarbeitung angeschlossenen Systemen
- Erweiterter Schutz vor unerwünschten Programmen durch Verwendung einer zentralen Softwareverteilung sowie Richtlinien zur Softwareinstallation
- Zentraler und dezentraler SPAM-Schutz
- Einsatz einer zentralen Firewall mit regelmäßigem Aktualisierungsintervall
- Zugriff auf das Netzwerk der OPTIMAL SYSTEMS GmbH nur für Berechtigte per SSL-VPN oder SSL gesicherter Terminal Server Verbindung
- Segmentierung des Netzwerks mit zwischengeschalteter Firewall
- Verschlüsselung von Notebooks, soweit technisch machbar
- Schutz von Geräte BIOS durch Passwortschutz, soweit technisch machbar
- Verwendung eines zentralen Patch Managements für die Verteilung von kritischen Patches zum Schutz vor Schwachstellen in der Datenverarbeitung angeschlossenen Systemen
- Wöchentliche, automatisierte Schwachstellenscans auf das Netzwerk der OPTIMAL SYSTEMS GmbH (Nessus Vulnerability Scanner)

2.3 Zugriffskontrolle

Die Zugriffskontrolle umfasst die Maßnahmen zur Verhinderung unerlaubter Tätigkeiten außerhalb der gewährten Berechtigungen.

- Zugriffberechtigungen sind im Berechtigungskonzept festgelegt
- Trennung der Berechtigungsbewilligung (organisatorisch) und der Berechtigungsvergabe (technisch)
- Wiederherstellung von Daten aus Backups ist geregelt (wer, wann, auf wessen Anforderung)
- Berechtigungen werden regelmäßig überprüft
- Protokollierung von Dateizugriffen, - veränderungen, -löschungen
- Verschlüsselte Speicherung von Daten gemäß Gefährdung
- Physische Löschung von Datenträgern oder Vernichtung durch qualifizierte Dienstleister
- Verwaltung von Benutzerrechten durch Administratoren
- Trennung von Arbeits- und Administrationsaccount

2.4 Auftragskontrolle

Die Maßnahmen sind bereits in dem Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit - Abschnitt 5.2.“ beschrieben.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Hier erfolgt die Auflistung zusätzlicher Maßnahmen hinsichtlich der Beauftragung von Unter-auftragnehmern im Sinne einer Verarbeitung im Auftrag.

- Sorgfältige Auswahl von Dienstleistern
- Kontrolle vorhandener Datensicherheitskonzepte
- Sichtung vorhandener IT-Sicherheitszertifikate der Dienstleister
- zentrale Erfassung vorhandener Dienstleister/Subunternehmen (zentrales Vertragsmanagement)
- Zugriff auf Kundendaten wird ausschließlich nach erfolgter Zustimmung gewährt.

2.5 Trennungskontrolle

Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, wird durch folgende Maßnahmen sichergestellt.

- Mandanten und rollenbasierte Zugangs- und Zugriffsberechtigung im firmeneigenen ECM-System enaio®
- Erteilung von Zugangs- und Zugriffsberechtigungen zweckgebunden an zuständige Mitarbeiter durch vordefinierte Abläufe
- Zugang und Zugriff auf Datenbestände der Kunden ausschließlich im Rahmen einer Vertragsbeziehung bzw. einer Einzelweisung

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

3 Pseudonymisierung und Verschlüsselung

Personenbezogene Daten werden im Wesentlichen zur Ausgestaltung von Kundenbeziehungen verwendet, die persönliche Kontakte voraussetzen. Häufig wird die Benennung von Ansprechpartnern für unterschiedliche Aufgabenstellungen vertraglich gefordert. In diesem Zusammenhang ist die Umsetzung einer Pseudonymisierung nicht möglich. Bei Datenzusammenstellungen jeglicher Art (z. B. Statistiken) werden im Zuge einer Datenminimierung personenbezogen Merkmale weitestgehend reduziert. Insgesamt wird die Pseudonymisierung damit als besondere Maßnahme des erweiterten Datenschutzes gemäß Kapitel 4.3 des Datenschutzkonzepts betrachtet und ggf. für konkrete Sachverhalte festgelegt.

Die Maßnahmen zur Verschlüsselung der Übertragung von personenbezogenen Daten werden in Abs. 4.1 beschrieben.

4 Maßnahmen zur Gewährleistung der Integrität

4.1 Weitergabekontrolle

Die Weitergabekontrolle umfasst die Maßnahmen zur Gewährleistung einer sicheren elektronischen Übertragung personenbezogener Daten bzw. eines sicheren Transports bzw. der Vernichtung von Datenträgern

- Dokumentation der Stellen, an die eine Übermittlung von Daten vorgesehen ist
- Übermittlung von Kundendaten erfolgt ausschließlich auf Basis vertraglicher Festlegungen bzw. auf dokumentierte Einzelweisung
- Elektronischer Transport personenbezogener Daten erfolgt ausschließlich auf verschlüsselten Datenträgern
- Verschlüsselter Austausch von Daten über (auf Anforderung des Kunden):
    - SSL-FTP-Server
    - Verschlüsselte E-Mails (S/MIME)
    - SSL gesichertem Filehosting (Nextcloud)
- Möglichkeit der digitalen Signierung von E-Mails mittels S/MIME

4.2 Eingabekontrolle

Alle vorhandenen Maßnahmen sind bereits in dem Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit“, Version 2.2 - Abschnitt 5.2. hinreichend beschrieben.

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

5 Verfügbarkeit und Belastbarkeit

5.1 Verfügbarkeitskontrolle

- Umfangreicher Schutz der produktionsrelevanten Server durch Nutzung eins professionellen Rechenzentrums
    - Redundante Stromversorgung
    - 10 Minuten USV Überbrückung beider Stromkreise
    - Netzersatzanlage mit 72 Stunden Kraftstoff Bevorratung
    - Kontrolle der Temperatur und Luftfeuchtigkeit im Rechenzentrum durch redundante Klimatisierung
    - Brandfrüherkennungssystem durch Rauchmelder mit automatischer Löschvorrichtung
    - Redundante Netzwerkanbindung
- Grundsätzliche Verwendung von redundanten Festplattensystemen für produktionsrelevante Systeme (min. RAID 1 / 5 / 10)
- Die Verfügbarkeit und ordnungsgemäße Funktion der zentralen IT-Systeme wird durchgehend durch ein Monitoring-System (Nagios) überwacht und im Fehlerfall ein Mitarbeiter benachrichtigt
- Backup- und Recovery-Konzept zur täglichen Sicherung der Produktivbereiche
    - Erstellung täglicher Off-Site Backups mit einer Aufbewahrungsdauer des Tages-Backups für 10 Tage, eines Wochenend-Backups für 5 Wochen, eines Monats-Backups für 12 Monate und eines Jahres-Backup für 2 Jahre
    - Die Off-Site Backups werden täglich AES-256 Bit verschlüsselt und auf zwei, bei Hetzner in getrennten Rechenzentren gehosteten von OPTIMAL SYSTEMS GmbH verwalteten Root-Servern mit redundantem Festplattensystem hochgeladen. Die Übertragung erfolgt SSH gesichert
    - Die Integrität der Backups wird wöchentlich mittels Prüfsummenabgleich sichergestellt
    - Der Backup-Vorgang wird protokolliert und täglich durch verantwortliche Mitarbeiter kontrolliert
    - Die für die Wiederherstellung notwendigen Backup-Keys werden nicht gemeinsam mit den Daten außerhalb der Räumlichkeiten der OPTIMAL SYSTEMS GmbH aufbewahrt und befinden sich zu keinem Zeitpunkt unverschlüsselt auf einem Datenträger
        - Für den Havariefall ist eine redundante, geschützte Aufbewahrung der Backup-Keys sichergestellt

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

  - Zur schnelleren Wiederherstellung werden zusätzlich zu den Off-Site-Backups tägliche lokale Backups auf dedizierten Festplatten-Arrays abgelegt. Die Aufbewahrungsdauer für diese Backups beträgt 30 Tage
- Für die zentralen IT-Systeme bestehen Wartungs- und Garantieverträge mit den jeweiligen Herstellern mit garantierter Wiederherstellung bei besonders kritischen Systemen

5.2 Wiederherstellbarkeit

Maßnahmen zur Gewährleistung einer raschen Wiederherstellung nach einem Störungsfall:

- Wiederanlaufplan für die Wiederinbetriebnahme der produktionsrelevanten Systeme
- Wiederherstellungsplan nach einer Havarie (Projekt in Realisierung bis Ende 2020)
- Die in 5.1 benannten Maßnahmen bezüglich Backups und Recovery, sowie Wartungs- und Garantieverträgen

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

6 Regelmäßige Überprüfung, Bewertung und Evaluierung

Regelmäßige Überprüfung der Einhaltung der DSGVO durch den Datenschutzbeauftragen.

Die OPTIMAL SYSTEMS GmbH hat einen Datenschutzbeauftragten gem. Art. 37 DSGVO i.V. m. § 38 BDSG benannt:

Stefan Eberle

von der Industrie- und Handelskammer
öffentlich bestellter und vereidigter Sachverständiger
für Telekommunikation und Verbindungspreisberechnung
sowie für Technik und Systeme der Informationsverarbeitung
Zuständige IHK: IHK Berlin

Hobeckweg 34
12623 Berlin
adv@optimal-systems.de
+49 30 895 708-0

Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de