OPTIMAL SYSTEMS

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

Version 1.2.2

Gültig ab: 29.01.2019

OPTIMAL SYSTEMS GmbH
Unternehmenszentrale
Cicerostrasse 26
10709 Berlin

Änderungsübersicht

Datum	Name	Änderung	Version
22.05.2018	Jasin Hahne	Erstellung	1.0
18.07.2018	G Wolf	Redaktionelle Korrekturen	1.2.0
06.09.2018	Alexander Tonn	Formelle Korrekturen	1.2.1
29.01.2019	Alexander Tonn	Änderung Datenschutzbeauftragter	1.2.2

Freigabeinformationen

Version	Erstellt durch	Erstelldatum	Unterschrift	Freigabe durch	Freigabedatum	Unterschrift
1.0	Jasin Hahne	22.05.2018	<digital>	Norbert Vogel	23.05.2018	<digital>
1.2.0	G Wolf	18.7.2018	<digital>	Gregor Wolf	18.7.18	<digital>
1.2.1	Alexander Tonn	06.09.2018	<digital>	Gregor Wolf	06.09.2018	<digital>
1.2.2	Alexander Tonn	29.01.2019	<digital>	Gregor Wolf	29.01.2019	<digital>

Inhaltsverzeichnis

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 bereits im Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit“, Version 2.0 – Abschnitt 5.2 angeführten Maßnahmen ergänzend dargelegt und vervollständigt.

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

2 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

2.1 Zutrittskontrolle

- Lage des Serverraum in einem von außen nicht zugänglichen Bereich des Gebäudes
- Zutritt zur sicheren Zone Serverraum ausschließlich für berechtigte Mitarbeiter durch Authentifizierung mittels RFID Schließanlage
- Wartungsarbeiten an Systemen der Datenverarbeitung grundsätzlich nur unter Aufsicht
- Bewegungsgesteuerte Videoüberwachung des Serverraum

2.2 Zugangskontrolle

- Verwendung von personalisierten Benutzerkennungen / Passwörtern
    - Die zu verwendenden Passwörter unterliegen technisch erzwungenen Richtlinien hinsichtlich der Komplexität, Änderungsintervallen, Passwortrotation und automatischer Sperrung bei Falscheingabe des Passwortes
- Zentraler und dezentraler Virenschutz an allen der Datenverarbeitung angeschlossenen Systemen
- Erweiterter Schutz von unerwünschten Programmen für Programmausführungsrichtlinien / AppWhitelisting (Projekt in Realisierung bis Ende Q3 2018)
- Zentraler und dezentraler SPAM-Schutz
- Einsatz einer zentralen Firewall mit regelmäßigen Aktualisierungsintervall

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

- 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 (Projekt in Realisierung bis Ende Q3 2018)
- Schutz von Geräte BIOS durch Passwortschutz, soweit technisch machbar
- Verwendung eines zentralen Patchmanagement 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

- Physische Löschung von Datenträger oder Vernichtung durch Externe
- Verwaltung von Benutzerrechten durch Administratoren
- Trennung von Arbeits- und Administrationsaccount

3 Pseudonymisierung und Verschlüsselung gem. Art. 32 Abs. 1 lit. a DSGVO

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

4 Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

4.1 Weitergabekontrolle

- Verschlüsselter Austausch von Daten über (auf Anforderung des Kunden):
  - SSL-FTP-Server
  - Verschlüsselte E-Mails (S/MIME)
  - SSL gesichertem Filehosting (Nextcloud)

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

- Verschlüsselte Datenträger

- 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 2.0 - Abschnitt 5.2.5 hinreichend beschrieben.

5 Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

5.1 Verfügbarkeitskontrolle

- Schutz der Anlagen zur Datenverarbeitung und Speicherung vor Blitzschäden durch zentrale VM (Überspannungs-) Ableiter, sowie vor Frequenzstörungen durch den Einsatz von Netzfiltern

- Kontrolle der Temperatur im Serverraum durch redundante Klimatisierung mit zwei unabhängigen Anlagen

- Überwachung von Temperatur und Luftfeuchtigkeit des Serverraum, einschließlich automatischer Benachrichtigung verantwortlicher Mitarbeiter, sobald ein Schwellwert überschritten, bzw. unterschritten wird

- Bewegungsgesteuerte Videoüberwachung des Serverraums

- Brandfrüherkennungssystem durch Rauchmelder mit automatischer Benachrichtigung der verantwortlichen Mitarbeiter

- 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

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

- Backup- und Recovery-Konzept zur täglichen Sicherung der Produktivbereiche
    - Erstellung täglicher Off-Site Backups mit Aufbewahrungsdauer des Tages-Backup für 10 Tage, eines Wochenend-Backup für 5 Wochen, eines Monats-Backup 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 dem 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
    - 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

6 Wiederherstellbarkeit der Verfügbarkeit bei einem Zwischenfall gem. Art. 1 lit c DSGVO

6.1 Wiederherstellbarkeit

Maßnahmen zur Gewährleistung einer raschen Wiederherstellung nach einem Störungsfall:

- Wiederanlaufplan für die wieder Inbetriebnahme der produktionsrelevanten Systeme
- Wiederherstellungsplan nach einer Havarie (Projekt in Realisierung bis Ende 2018)

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

- Die in 5.1 benannten Maßnahmen bezüglich Backup und Recovery, sowie Wartungs- und Garantieverträgen

7 Zweckbindung gem. Art. 5 Abs. 1 lit. B DSGVO

7.1 Trennbarkeit

Alle vorhandenen Maßnahmen sind bereits in dem Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit“, Version 2.0 - Abschnitt 5.2.8 hinreichend beschrieben.

8 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 1 lit d DSGVO

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
+4930 895 708 0

9 Auftragskontrolle

Alle vorhandenen Maßnahmen sind bereits in dem Datenschutzkonzept „Datenschutzkonzept - Unternehmenserklärung zum Datenschutz und Datensicherheit - Abschnitt 5.2.6“ 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