Beschreibung der technischen und organisatorischen Maßnahmen

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO):

Verantwortlicher:

SkySystems IT GmbH

Oeger Straße 47, 58642 Iserlohn (Deutschland)

Tel: 02374409480, E-Mail: info@skysystems.it, Web: www.skysystems.it

Gesetzlicher Vertreter:

Roger Geitzenauer

Datenschutzbeauftragter:

Jörg Stockmann - Avallon GmbH

Tel: 049419839070

E-Mail: dsb@avallon.de

Übersicht der technischen und organisatorischen Maßnahmen

TOM SkySystems IT global..... 3

TOM SkySystems IT global

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Alarmanlage mit Meldung an Sicherheitsdienst [umgesetzt]
- Chipkarten - Chipkarten-/Transponder-Schließsystem [umgesetzt]
- Empfang - Besucherkontrolle am Eingang [umgesetzt]
- Manuelles Schließsystem - Manuelles Schließsystem mit Schließzylinder [umgesetzt]
- Schlüsselverwaltung - Schlüsselvergabe und -management erfolgen nach einem definierten Prozess [umgesetzt]
- Videoüberwachung - Videoüberwachung aller Zugänge [umgesetzt]

Die Maßnahmen Alarmanlage und Videoüberwachung erfolgen nur am Standort Letmathe.

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzererkennung und Passwort [umgesetzt]
- Benutzerberechtigungen - Berechtigungsmanagement mit Prozessen für Zuweisung, Entzug und Kontrolle von Rechten [umgesetzt]
- Firewall - Einsatz von Firewalls zum Schutz von Netzwerken und Systemen [umgesetzt]
- MDM - Einsatz von Mobile Device Management [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellung und Einsatz eines Berechtigungskonzepts [umgesetzt]
- Datenlöschung - Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben) [umgesetzt]

Beschreibung der technischen und organisatorischen Maßnahmen

- Einsatz von Aktenvernichtern - Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2) [umgesetzt]
- Passwortrichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung - E-Mail-Verschlüsselung mit dem Stand der Technik entsprechenden Verfahren
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet [umgesetzt]
- VPN-Tunnel - Einsatz von VPN-Technik für externe Zugriffe auf interne Ressourcen [umgesetzt]

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig) [umgesetzt]

M.1.6 Beschreibung der Pseudonymisierung:

Durchführen von Maßnahmen zur Pseudonymisierung, sofern möglich.
Verschlüsselung von Daten als technische Alternative zur Pseudonymisierung.

M.1.7 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES-256 Standard) [umgesetzt]
- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mail-Verschlüsselung nach S/MIME, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL) [umgesetzt]

M.1.8 Beschreibung der Datenträgerkontrolle:

- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]
- Vernichtung - Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) [umgesetzt]
- Verschlüsselung - Verschlüsselung von mobilen Datenträgern [umgesetzt]

M.1.9 Beschreibung der Benutzerkontrolle:

- Passwortvergabe - Schutz der Benutzerkonten durch Passwörter [umgesetzt]
- Sperrung von Ex-Mitarbeiter - Sperren von Benutzerkonten ausgeschiedener Mitarbeiter [umgesetzt]
- Zweifaktor-Authentifizierung - Authentifikation mit Benutzername, Passwort und einem zweiten Faktor (z.B. Hardwaretoken, SMS) [umgesetzt]

M.1.10 Beschreibung der Übertragungskontrolle:

- Protokollierung - Protokollierung aller Übertragungsvorgänge [umgesetzt]

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzerkennungen (nicht Benutzergruppen) [umgesetzt]
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten [umgesetzt]
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe [umgesetzt]

M.2.2 Beschreibung der Datenintegrität:

- Datensicherungskonzept - Erstellen eines Backup- und Recoverykonzeptes [umgesetzt]

M.2.3 Beschreibung der Speicherkontrolle:

- Berechtigungskonzept - Festlegung von Berechtigungen in einem Berechtigungskonzept [umgesetzt]
- Need-to-Know Prinzip - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert [umgesetzt]

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware [umgesetzt]
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort [umgesetzt]
- Backup- und Recoverykonzept - Umsetzung eines Backup- und Recoverykonzeptes [umgesetzt]
- Feuerlöschgeräte - Feuerlöschgeräte in Server-/Verteilerräumen [umgesetzt]
- IT-Notfallplan - Erstellung und Anwendung von IT-Notfallplänen [umgesetzt]

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen [umgesetzt]
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne [umgesetzt]

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Auswahl - Auswahl von Auftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [umgesetzt]
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO [umgesetzt]
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- DSB - Benennung eines Datenschutzbeauftragten [umgesetzt]
- Incident-Response-System - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Managementsystem Datenschutz - Managementsystem zum Datenschutz (z.B. in Anlehnung an ISO 27701)
- Managementsystem Informationssicherheit - Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 10000) [umgesetzt]
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter; regelmäßig stattfindende Nachschulungen.
- Schwachstellenanalysen - Durchführung regelmäßiger Schwachstellen-Tests [umgesetzt]
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. Art. 25 Abs. 2 DS-GVO
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. Ligatur) [umgesetzt]
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO [umgesetzt]

M.4.3 Beschreibung der Organisationskontrolle:

- Datenschutzbeauftragter - Ein Datenschutzbeauftragter ist benannt, gemeldet und seine Kontaktdaten sind veröffentlicht. [umgesetzt]
- Dokumentation der Verarbeitung - Alle Verarbeitungstätigkeiten sind dokumentiert und werden regelmäßig überprüft.
- Richtlinien - Es existieren verbindliche Richtlinien für den Umgang mit personenbezogenen Daten. [umgesetzt]
- Sensibilisierung - Mitarbeiter werden regelmäßig zum Datenschutz sensibilisiert und geschult.