UNITED SIGNALS

Technische & Organisatorische Maßnahmen nach Art. 3 DSV (Art 32 DSGVO)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1. Vertraulichkeit

1.1 Zutrittskontrolle

→ Kein unbefugter Zutritt zu Datenverarbeitungsanlagen (Gebäude- und Raumsicherung):

☐ Magnet- oder Chipkarten
☒ Schlüssel
☒ elektrische Türöffner
☒ Werkschutz bzw. Pförtner
☒ Alarmanlagen
☒ Videoanlagen
☐ Automatisches Zugangskontrollsystem
☐ Schließsystem mit Codesperre
☐ Manuelles Schließsystem
☒ Sicherheitsschlösser
☒ Schlüsselregelung (Schlüsselausgabe etc.)
☐ Biometrische Zugangssperren
☐ Protokollierung der Besucher
☒ Sorgfältige Auswahl von Reinigungspersonal
☒ Sorgfältige Auswahl von Wachpersonal
☐ Tragepflicht von Berechtigungsausweisen
☒ Besucher werden beaufsichtigt
☒ Jeder kennt jeden (KMU)
☒ Zutrittsberechtigungsstruktur ist auf das Notwendigste beschränkt

1.2 Zugangskontrolle

→ Keine unbefugte Systembenutzung:

☒ (sichere) Kennwörter
☒ automatische Desktopsperre
☒ Erstellen und Einsatz einer Password Policy
☒ Zwei-Faktor-Authentifizierung

☒ Verschlüsselung von Datenträgern
☒ Zuordnung von Benutzerrechten
☒ Erstellen von Benutzerprofilen
☒ Authentifikation mit Benutzername / Passwort
☐ Gehäuseverriegelungen
☐ Einsatz von VPN-Technologie
☒ Sperren von externen Schnittstellen (USB etc.)
☐ Verschlüsselung von mobilen Datenträgern
☐ Verschlüsselung von Smartphone-Inhalten
☐ Einsatz von zentraler Smartphone-Administrations-Software
☒ Einsatz von Anti-Viren-Software
☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
☐ Einsatz einer Hardware/Software-Firewall
☒ Zutrittsberechtigungsstruktur ist auf das Notwendigste beschränkt

1.3 Zugriffskontrolle

→ Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

☒ Erstellen und Einsatz Berechtigungskonzepte sowie bedarfsgerechte Zugriffsrechte
☒ Protokollierung von Zugriffen auf Anwendungen: Eingabe, Änderung und Löschung
☒ Verwaltung der Rechte durch Systemadministrator
☒ Reduzierung der Anzahl der Administratoren
☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒ Sichere Aufbewahrung von Datenträgern
☒ Sicheres Wipen von Datenträgern vor Wiederverwendung
☒ Ordnungsgemäße Vernichtung von Datenträgern

1.4 Trennungskontrolle

→ Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒ Trennung von Produktiv- und Testumgebung
☒ Softwarebasierte Mandantentrennung
☒ Erstellung eines Berechtigungskonzepts
☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☒ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei
☒ Festlegung von Datenbankrechten

1.5 Pseudonymisierung

☐ Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität

2.1 Weitergabekontrolle

→ Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

☐ E-Mail-Verschlüsselung
☐ Virtual Private Networks (VPN)
☐ elektronische Signatur
☒ Protokollierung der Zugriffe und Abrufe
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https
☒ Weitergabe von personenbezogenen Daten in anonymisierter oder pseudonymisierter Form
☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
☐ Beim physischen Transport: sichere Transportbehälter /-verpackungen

2.2 Eingabekontrolle

→ Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

☒ Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten
☒ Dokumentenmanagement
☒ Erstellen einer Übersicht, mit welchen Applikationen welche personenbezogenen Daten eingegeben, geändert und gelöscht werden können.
☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten durch individuelle Benutzernamen
☐ Aufbewahrung von Formularen, von denen personenbezogene Daten in automatisierte Verarbeitungen übernommen worden sind
☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung personenbezogener Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

→ Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

(Hinweis: United Signals betreibt selbst keine Server, daher gibt es auch keine Server-Infrastruktur zu schützen. Wir nutzen SaaS Lösungen, die von Drittanbietern verwaltet werden. Daher beziehen sich die Antworten in diesem Abschnitt auf die Lösungen unserer Drittanbieter)

☒ Backup-Strategie (online/offline; on-site/off-site)
☒ unterbrechungsfreie Stromversorgung (USV)
☒ Virenschutz
☒ Firewall

- ☒ Meldewege und Notfallpläne
- ☒ Rasche Wiederherstellbarkeit
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ RAID-System / Festplattenspiegelung
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Videoüberwachung Serverraum
- ☒ Serverraumüberwachung Temperatur und Feuchtigkeit
- ☒ Erstellen eines Backup-Konzepts
- ☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management

- ☒ Software-Lösungen für Datenschutz-Management im Einsatz
- ☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)
- ☒ Sicherheitszertifizierung nach SOC2
- ☒ Anderweitiges dokumentiertes Sicherheitskonzept
- ☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- ☒ externer Datenschutzbeauftragter
- ☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- ☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
- ☒ Interner / externer Informationssicherheitsbeauftragter
- ☒ Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)
- ☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- ☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

- ☒ Einsatz von Firewall und regelmäßige Aktualisierung
- ☒ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ☒ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ☒ Intrusion Detection System (IDS)
- ☒ Intrusion Prevention System (IPS)
- ☒ regelmäßige Software-Updates (Patch- und Schwachstellenmanagement)
- ☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen /Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

☒ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4 Auftragskontrolle (Outsourcing an Dritte)

☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
☒ Schriftliche Weisungen an den Auftragnehmer
☒ Eindeutige Vertragsgestaltung
☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☒ Regelung zum Einsatz weiterer Sub-Unternehmer
☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus