Stand: 01.12.2023

Allgemeine Beschreibung zu den Maßnahmen nach Art. 32 DSGVO

Das Unternehmen synaforce GmbH (ehemals Hartl Group GmbH) in Hofkirchen ist seit dem Jahr 2009 nach der ISO IEC 27001 zertifiziert. Dabei handelt es sich um eine international anerkannte IT-Zertifizierung bei der das Informationssicherheitsmanagementsystem (ISMS) an oberster Stelle steht. Nicht das Vorhandensein, sondern die Wirksamkeit dieses ISMS wird jährlich durch die unabhängige Zertifizierungsstelle TÜV Rheinland überprüft. Zusätzlich werden regelmäßig interne Audits durch den Informationssicherheitsbeauftragten und den internen Datenschutzbeauftragten (DSB) durchgeführt

Der Vorteil dieser Norm ist der „ganzheitliche Ansatz“. Die Erfüllung der datenschutzrechtlichen Anforderungen nach der EU-Datenschutz-Grundverordnung (DSGVO) sowie die Umsetzung des IT-Grundschutzes gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen nur einzelne Teile der Anforderungen dar. Umgebungssicherheit, Gebäudeschutz wie Zutrittskontrolle und technische Sicherheit, aber auch organisatorische Maßnahmen wie regelmäßige Weiterbildung der Mitarbeiter in Datenschutz-, IT-Sicherheits- und IT-Technischen Themen müssen berücksichtigt werden.

Einige Beispiele zu technischen Maßnahmen:

Zur **Gebäudeüberwachung** kommen eine Alarmanlage mit Bewegungs- und Rauchmeldern, sowie eine Videoüberwachung zum Einsatz. Alle Anlagen unterliegen durch geplante, interne Audits einer ständigen Kontrolle durch den Informationssicherheitsbeauftragten.

Stromunterbrechungen werden im ersten Moment durch zwei USV-Anlagen je 80 kVA (in separaten Brandabschnitten) abgefangen bis dann eines der zwei redundanten Notstrom-Dieselaggregate die Stromproduktion übernimmt. Die Leistung der eigenen Energieversorgung reicht zum Weiterbetrieb des kompletten Rechenzentrums aus.

Auch die **Klimatisierung** des Serverraums ist ausreichend abgesichert. Die Kühlung erfolgt durch drei redundante Klimaanlagen, die den Ausfall einer Anlage komplett ausgleichen können und die komplette Kühlung des Serverraums gewährleisten.

Die **Datensicherung** aller System- und Anwendungsdaten auf den gehosteten Systemen übernimmt die synaforce GmbH. Die synaforce GmbH sichert abhängig vom jeweiligen Sicherungszyklus und vorbehaltlich abweichender Vereinbarungen nach Maßgabe der Sicherungsstrategie der synaforce GmbH voll, inkrementell oder auch differenziell diese System- und Anwendungsdaten je einmal werktäglich, d.h. einmal an jedem Kalendertag von Montag bis Freitag. Diese System- und Anwendungsdaten werden für einen Zeitraum von 30 Kalendertagen als Tagessicherungen aufbewahrt. Die letzte Tagessicherung im Monat wird für weitere zwei Monate vorgehalten. Um der synaforce GmbH die ordnungsgemäße Durchführung zu ermöglichen, muss der Auftraggeber der synaforce GmbH die notwendigen Zugriffsrechte für die Dauer der Vereinbarung gewähren. Die Backups werden auf einen hochverfügbaren, vor unbefugter Manipulation durch Dritte (z.B. durch Ransomware) geschützten und verschlüsselten Backupspeicher geschrieben und über zwei Rechenzentren mit einer Distanz von mindestens 150 km synchron gehalten.

Im Notfall stehen **Backup-Ressourcen** an anderen Standorten zur Verfügung.

System- und Netzwerkkontrolle

Im Bereich der synaforce GmbH wird die System- und Netzwerkkontrolle durch eigene Mitarbeiter durchgeführt. Details regelt die „SOP* 10 System- und Netzwerkkontrolle“ welche besagt, dass:

- zur Überwachung das Produkt PRTG eingesetzt wird

- Systeme 7/24 überwacht werden
- Systeme mit einer Vielzahl von Sensoren überwacht werden können
  Beispiel: Ping, CPU-Auslastung, Speicherplatzbelegung, Arbeitsspeicherauslastung, uvm.
- eine automatische Alarmierung bei Grenzwertüberschreitung erfolgt

Updates

Die synaforce GmbH setzt zur Aktualisierung ihrer Systeme einen WSUS-Server ein. Dieser stellt sicher, dass wichtige Aktualisierungen zeitnah übernommen werden. Vor der Installation auf allen betroffenen Systemen wird eine Testgruppe aktualisiert, um fehlerhafte Updates frühzeitig zu identifizieren. Details regelt die „SOP* 07 Patchmanagement“ welche besagt, dass:

- Updates gruppenbasiert verteilt werden
- zuerst eine Testgruppe aktualisiert wird
- es eine Gruppe für automatische Installation und eine für manuelle Installation gibt
- Updates auf Livesystemen 1 Woche nach Freigabe durch den Hersteller installiert werden (Sicherheitswartezeit)

Virenschutz

Die synaforce GmbH setzt zum Virenschutz ein aktuelles Produkt eines namhaften Herstellers ein. Mehrmals täglich werden aktuelle Virensignaturen bereitgestellt was die Wirksamkeit der Schutzsoftware erheblich steigert. Details sind in der „SOP* 08 Virenschutz“ geregelt, welche besagt, dass:

- die Verteilung der Schutzsoftware automatisch erfolgt
- unterschiedliche Versionen / Konfigurationen für Workstations, Server definiert sind
- bei Virenbefall die vorgegebenen Schritte einzuhalten sind

Einige Beispiele zu organisatorischen Maßnahmen:

Alle **Geschäftsprozesse**, bei denen schutzwürdige Daten verarbeitet werden, wurden betrachtet und dokumentiert. Zusammengefasst werden sie in Standard Operating Procedures (SOP´s) und als solche unterliegen sie der Dokumentenlenkung nach ISO-Vorgaben, die neben der Versionierung und Änderungshistory auch die regelmäßige Kontrolle und Überarbeitung fordert.

Geplante Änderungen (Change) an IT-Systemen unterliegen dem „Change Control System“. Dadurch müssen geplante Änderungen schriftlich beantragt und genehmigt (4-Augen-Prinzip) werden, wobei durch jeden Prozessteilnehmer eine Risikobewertung durchzuführen und zu dokumentieren ist. Große Änderungen bedürfen einer zweiten genehmigenden Person und erfahren dadurch eine erweiterte Risikobewertung.

Der gesamte Prozess wird nachvollziehbar in Multidata** festgehalten. Details regelt die „SOP* 06 Change Control“ welche besagt, dass:

- Änderungen klassifiziert werden müssen nach geringen, mittleren und großen Änderungen
- jede geplante Systemänderung schriftlich via Change Control beantragt werden muss
- ungeplante Änderungen z.B. Störungsbehebungen von dieser Regelung ausgenommen sind
- der Change-Prozess in MD** abgebildet ist

Aufgabengebiete sind klar getrennt und werden von einem Hauptverantwortlichen, sowie mindestens einem Vertreter betreut. Dieser übernimmt die Aufgaben aber nicht nur bei Abwesenheit des Hauptverantwortlichen, sondern in ständigem, planmäßigem Wechsel um die jeweilige Fachkompetenz zu erhalten und zu fördern.

*Standard Operating Procedure, ** ERP und CRM System der synaforce GmbH

TOM gemäß Artikel 32 DSGVO:

Zutrittskontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Eingangstür/Zufahrtstor immer verschlossen, Zutritt nur mittels RFID-Chip oder Schließanlagenschlüssel
- Empfang ist während der Arbeitszeiten besetzt
- Bürotüren sind mit elektronischen Türschlössern gesichert und können nur bei entsprechender Berechtigung geöffnet werden
- Rechenzentrum durch Sicherheitsschleuse und Stahltüren mit elektronischem Fingerprintleser gesichert
- Gebäude durch Alarmanlage gesichert
- Gebäude und Gelände wird per Video überwacht
- SOP Zutrittskontrolle

Zugangskontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Unbefugten ist die Nutzung von Datenverarbeitungssystemen zu verwehren.

- AD-Authentifizierung an allen DV-Systemen
- Verschlüsselung von mobilen Geräten
- regelmäßiger Passwortwechsel mit Windows - Kennwortrichtlinie
- Externer Zugriff ausschließlich über Zwei-Faktor-Authentifizierung

Zugriffskontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Berechtigten ist ausschließlich der Zugriff auf die ihrer Zugriffsberechtigung entsprechenden Daten zu gewähren.

- Berechtigungskonzept mit regelmäßiger Kontrolle durch internes Audit
- Rechtesteuerung durch die Personalverwaltung
- SOP Zugriffskontrolle

Auftragskontrolle (Art. 32 Abs. 1 lit. D, Art. 25 Abs. 1 DSGVO)
Daten, die im Auftrag verarbeitet werden dürfen, nur den Weisungen des Auftraggebers entsprechend verarbeitet werden.

- Verfahrensanweisungen gem. ISO 27001 und ISO 9001
- Vertraglich fixierte Auftragsdatenverarbeitung
- Regelmäßige Weiterbildung der Mitarbeiter
- regelmäßige Kontrollen durch interne und externe Audits

Eingabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Es muss feststellbar sein, ob und von wem personenbezogene Daten in DV-Anlagen eingegeben, geändert oder entfernt wurden.

- AD-Authentifizierung an allen DV-Systemen
- Log-Datei Erstellung mit zentraler Archivierung
- Change Management System gem. ISO 27001
- werktägliche Datensicherung
- Netzwerküberwachung

*Standard Operating Procedure, ** ERP und CRM System der synaforce GmbH

Weitergabekontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Daten dürfen während der elektronischen Übertragung oder während ihres Transportes nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Regelungen zur Nutzung von Internet und E-Mail
- verschlüsselte Datenübermittlung
- Netzwerksicherheit durch Hard- und Software Sicherheitskomponenten
- Verschlüsselung von mobilen Geräten und Datenträgern
- Geheimhaltungserklärung intern / extern
- Dienstanweisung

Verfügbarkeitskontrolle (Art. 32 Abs. 1 lit. b DSGVO)
Daten müssen vor zufälliger Zerstörung und Verlust geschützt werden.

- werktägliche Datensicherung
- Gebäude durch Alarmanlage gesichert
- Zutrittsschutz
- Brandfrüherkennung und Löschanlage im Rechenzentrum
- Notfallpläne gemäß ISO 27001
- unterbrechungsfreie Stromversorgung und zwei Diesel-Notstromaggregate
- ständige Netzwerküberwachung
- regelmäßige Kontrollen durch interne und externe Audits

Gebot der Datentrennung (Art. 32 Abs. 1 lit. b DSGVO)
Daten die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden können.

- Einsatz von Standardsoftware und -datenbanksystemen
- getrennte IT-Netzwerke (Kunden, Management, Test, usw.)

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- werktägliche Datensicherung
- regelmäßige Wiederherstellungstests

Datensicherheitsmanagement (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)
Verfahren, die eine regelmäßige Überprüfung, Auswertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gewährleisten

- Incident-Response-Management: Wird über Meldezentrale (Sicherheitsvorfälle) im SharePoint erfasst, durch die Verantwortlichen kategorisiert und dann über das Ticketsystem abgearbeitet.
- jährliche externe Audits zu ISO9001, ISO27001, DIN EN 50600 CAT III
- jährliche externe Audits zu ISAE 3402 Type II
- regelmäßige interne Audits zu Datenschutz und IT- und Informationsicherheit durch ISB und DSB

Weiterführende Infos und Dokumente:

Unsere **Zertifikate** und eine **ausführliche Beschreibung unserer Technischen und Organisatorischen Maßnahmen** können Sie im Downloadbereich unserer Internetseite einsehen und herunterladen.

Downloadbereich: https://www.synaforce.com/downloads

*Standard Operating Procedure, ** ERP und CRM System der synaforce GmbH