Anlage Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Zutrittskontrolle

Der Zutritt zu den Büros und Serverräumen erfolgt über Magnetkarten des Typs Legic.

Die dazugehörigen Berechtigungen werden durch die Personalabteilung innerhalb des Systems Interflex gepflegt und vergeben.

Anforderungen für die Vergabe von Berechtigungen werden durch den zuständigen Abteilungsleiter freigegeben.

Zur Zutrittskontrolle befinden sich Terminals des Typs Pegasys, Interflex IF5735, IF700, IF603, IF610, W02 und Bezeichnung der Berliner Systeme im Einsatz. Weiterhin sind Elektronische Türgriffe TSE 4001 der Marke Burgwächter im Einsatz.

Das Geschehen auf dem Gelände und in den Serverräumen wird mittels Videoüberwachung rund um die Uhr aufgezeichnet und für Kontrollzwecke maximal 90 Tage vorgehalten.

Zusätzlich sorgt der beauftragte Sicherheitsdienst für Kontrollgänge, die entsprechend dokumentiert werden und überwacht sämtliche Zugänge des Werksgeländes. Das Pförtnerhaus ist rund um die Uhr durch Personal des Sicherheitsdienstes besetzt.

Die Vergabe von Schlüsseln erfolgt auf Anforderung der verantwortlichen Abteilungsleiter, wird durch die Personalabteilung vorgenommen und in einem Schlüsselbuch dokumentiert.

2. Zugangskontrolle

Der Zugang zu den IT-Systemen erfolgt grundsätzlich im ersten Schritt über die Anmeldung im Windows Active Directory mit entsprechendem Benutzernamen und Kennwort.

Dort gibt es pro User genau einen Benutzerstammsatz. Die Passwortrichtlinien werden gemäß aktuellem IT-Grundschutz-Kompendium vom BSI umgesetzt und durch die Active Directory im gesamten Netzwerks überwacht.

Darüber hinaus kann sich der Nutzer zur Verarbeitung von Daten im SAP System anmelden. Dort hat der User einen weiteren Benutzerstammsatz mit einer separaten Kennwortvergabe. Diese ist unabhängig vom Windows Active Directory.

In der Oracle basierenden Produktionsdatenbank ist ebenfalls eine gesonderte Benutzeranmeldung erforderlich, auch diese ist unabhängig von der Anmeldung in der Windows Active Directory.

Das Mailsystem in der HCL Notes/Domino-Umgebungen ist durch Anmeldename und Kennwort gegen unbefugte Benutzung abgesichert.

3. Zugriffskontrolle

Für die Arbeit im SAP System ist ein Rollenmodell hinterlegt. Dies stellt sicher, dass der jeweilige Mitarbeiter nur Zugriff auf die für seine Arbeit erforderlichen Daten hat. Änderungen werden separat über das Ticketsystem und die Freigabe des verantwortlichen Abteilungsleiters durchgeführt und sowohl im Ticketsystem als auch im SAP System protokolliert.

4. Weitergabekontrolle

Der Dateneingang erfolgt grundsätzlich auf unserem FTP Server in der DMZ. Von dort werden diese automatisiert an das SAP System zur Auftragsanlage übergeben. Es findet kein Transport mit physischen Medien statt. Zu jedem Zeitpunkt ist der Zugriff nur über die entsprechenden Benutzernamen und Kennwörter möglich.

Die Ablage und der Transfer der Daten werden protokolliert.

5. Eingabekontrolle

Die Protokollierung aller Eingaben erfolgt automatisch im SAP System mit Benutzername, Datum und Uhrzeit.

6. Auftragskontrolle

Die Verarbeitung von Auftraggeberdaten erfolgt gemäß den Weisungen aus dem AV-Vertrag und ggf. auf Grundlage dokumentierter Einzelweisungen. Weisungen werden grundsätzlich schriftlich erteilt oder schriftlich / in Textform bestätigt.

Vor der Beauftragung von Unterauftragnehmern (bzw. sonstigen externen Dienstleistern) erfolgt eine Bewertung hinsichtlich ihrer Eignung. Unterauftragnehmer werden sorgfältig ausgesucht und regelmäßig kontrolliert.

7. Verfügbarkeitskontrolle

Die Daten werden in zwei getrennten Rechenzentren am Standort Röbel gespeichert. Diese befinden sich in unterschiedlichen Brandabschnitten. Innerhalb der Rechenzentren erfolgt die Datenspeicherung mittels RAID-DP auf NetApp Storage. Dieser ist hochverfügbar im Metrocluster über beide Rechenzentren gespiegelt. Backups für alle Systeme und Speicherbereiche werden mittels IBM Tivoli Storage Manager auf Tape durchgeführt. Die Tapes befinden sich in vollautomatischen Qualstar Libraries.

Die in den Rechenzentren angeschlossenen Systeme sind einerseits über USV abgesichert und parallel an das Stromnetz direkt angeschlossen. Damit wird sichergestellt, dass ein Ausfall der USV keine Auswirkungen hat, solange gleichzeitig das öffentliche Stromnetz verfügbar ist.

Der Zugriff vom und in das Internet wird mittels DMZ und Firewalls der Firma Checkpoint abgesichert. Ein direkter Zugriff von außen auf das ERP-System ist nicht möglich.

Wir setzen als End-Point-Security-Lösung Kaspersky in der Business-Select Version ein. Zusätzlich läuft auf den Mail-Servern Avira zur Erkennung von Viren, Trojanern und Malware.

8. Trennungskontrolle

Das physische Netzwerk ist in mehrere Subnetze aufgeteilt, um den Datenfluss von Maschinen sowie Produktions- und Mandantendaten zu trennen. Auftragsdaten werden in unserem CRM-Programm nach Kunden getrennt abgespeichert. So wird sichergestellt, dass auch nur die für den jeweiligen Auftrag bzw. Mandanten erforderlichen Daten zur Verfügung gestellt werden. Mittels Rollen im Berechtigungskonzept ist sichergestellt, dass die Nutzer nur die für ihre Aufgaben erforderlichen Daten einsehen oder bearbeiten können.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DS-GVO)

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO)
- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Betroffenen (Art. 34 DS-GVO).

Dr. Peter Runge
Leitung Produktion & Logistik
Prokurist