Das ERP für Maschinen- und Anlagenbau!

IT Sicherheits-Konzept

Technische und organisatorische Maßnahmen des Auftragsverarbeiters gem. Art. 32 DSGVO. Sicherheit der Verarbeitung

Unternehmen	Leitung des Unternehmens
schrempp edv GmbH Rainer-Haungs-Straße 7 77933 Lahr	Brigitta Schrempp Stefan Basler
Leitung der Datenverarbeitung	**Datenschutzbeauftragter**
Franz Kempf	Herbert C. Huber Kleinoberfeld 7 76135 Karlsruhe

Art. 32 DSGVO - Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig,oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

1 VERTRAULICHKEIT

Die Vertraulichkeit der Datenverarbeitung wird durch die folgenden Maßnahmen gesichert.

1.1 Zutrittskontrolle

Der Auftragnehmer gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, auf der die personenbezogenen Daten verarbeitet oder genutzt werden, verwehrt wird. Dies geschieht durch:

- Alarmanlage
- Persönliche Überwachung
- Besetzter Empfang
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe)
- Sorgfältige Auswahl des Reinigungspersonals
- Zutritt zum Gebäude und allen relevanten Räumen nur für Berechtigte, d.h. die jeweiligen Mitarbeiter, Besucher nur in Begleitung von berechtigten Mitarbeitern

1.2 Zugangskontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen, dass seine Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen. Dies geschieht durch:

- Zuordnung von Benutzerrechten
- Passwortvergabe, Passwortsicherheit u.a. Mindestlänge
- Einsatz von VPN-Verbindungen
- Einsatz von Antivirensoftware
- Erstellen von Benutzerprofilen
- Authentifizierung mit Benutzername und Passwort
- Sperren bestimmter Ports
- Einsatz von Intrusion-Detection-Systeme
- Einsatz einer Hardwarefirewall

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

- Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls
- Berechtigungskonzept
- Anzahl Administratoren so gering wie möglich
- Physische Löschung von Datenträgern vor Wiederverwendung
- Sichere Aufbewahrung von Datenträgern (Datensicherungsfestplatten)
- Rechteverwaltung durch Administrator
- Einsatz von Aktenvernichtern/Dienstleister
- Ordnungsgemäße Vernichtung von Datenträgern

1.4 Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Getrennte Verarbeitung zweckgebundener Daten
- Die Daten unterschiedlicher Auftraggeber / Projekte werden soweit möglich auf unterschiedlichen Systemen verarbeitet
- Funktionstrennung von Produktiv- und Testsystem

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugeordnet werden.(Art. 4 Nr. 5 DS-GVO).

Prozesse, die mit personenbezogenen Daten arbeiten, sind bereits von Anfang an datenschutzfreundlich zu gestalten; die Pseudonymisierung kann hierfür ein wichtiger Bestandteil sein.

Maßnahmen zur Pseudonymisierung personenbezogener Daten

a) Trennung von Kundenstammdaten und Kundenumsatzdaten
b) Verwendung von Personal-, Kunden-, Lieferanten-Kennziffern statt Namen

2 INTEGRITÄT

Die Integrität der Daten wird durch folgende Maßnahmen sichergestellt:

2.1 Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Protokollierung von Stammdatenänderungen
- Vergabe von Änderungs-, Lösch- und Bearbeitungsrechten aufgrund eines Rollenberechtigungskonzeptes
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung der Serveraktivitäten
- Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer

2.2 Weitergabekontrolle

Bei der Weitergabekontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies geschieht durch:

- Sichere Löschung von Datenträgern
- VPN-Tunnelverbindung bei externen Geräten
- Verbot der Nutzung privater Datenträger am Arbeitsplatz
- Sorgfältige Auswahl von Transportpersonal

2.3 Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

- Auftragnehmer hat Datenschutzbeauftragten benannt
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Kontrollrechte gegenüber dem Auftragnehmer
- Laufende Kontrolle des Auftragnehmers
- Schriftliche Weisungen an den Auftragnehmer
- Sicherstellung der Vernichtung von Daten nach Vertragsende
- Verpflichtung der Mitarbeiter des Auftragnehmers auf den Datenschutz / Verschwiegenheitspflichten
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

3 VERFÜGBARKEIT UND BELASTBARKEIT

Die Schutzziele Verfügbarkeit und Belastbarbarkeit werden durch die folgenden Maßnahmen sichergestellt:

3.1 Verfügbarkeitskontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen die unbeabsichtigte Zerstörung oder den Verlust personenbezogener Daten. Dies geschieht durch:

- Klimaanlage in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherungen im anderem Brandabschnitt
- Virenschutz und Firewall-Konzepte
- Unterbrechungsfreie Stromversorgung (USV)
- geregeltes Backup Verfahren
- HA – System über mehrere Brandabschnitte
- Spiegelung von Festplatten (RAID) Systeme, VM System
- Regelmäßige Erstellung von Sicherheitskopien
- Erstellen eines Notfallplans
- geregeltes Backup- und Recoverykonzept
- Überspannungsfilter

4 VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

Ein regelmäßiges Kontroll- und Evaluierungskonzept wird wie folgt umgesetzt:

- Regelmäßige Mitarbeiterschulungen- und Prüfungen
- Regelmäßiges Einspielen von Patches und Softwareupdates
- Jährliches Datenschutz-Audit
- Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recovery-Konzeptes im Serverbereich

Die schriftliche Dokumentation beinhaltet:

- Interne Verhaltensregeln
- Datensicherheitsbeschreibung
- Risikoanalyse
- Datensicherungs-Konzept

Verantwortlicher für die Erstellung **Huber, Datenschutzbeauftragter**