

1. **Pseudonomisierung**  
HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport)
2. **Zutrittskontrolle**  
Alarmanlage, Videoüberwachung  
Personenkontrolle  
Sicherheitsschlösser, dokumentierte und nachprüfbare Schlüsselregelung  
Gesicherter Eingang für An- u. Ablieferungen  
Bewegungsmelder  
Durchgängig geschlossene Produktionsräume
3. **Zugangskontrolle**  
Zuordnung von Benutzerrechten  
Passwortvergabe  
Schlüsselregelung  
Einsatz von Anti-Viren-Software  
Einsatz einer physisch getrennten Firewall  
Erstellen von Benutzerprofilen und Zuordnung von Benutzerprofilen zu IT-Systemen
4. **Zugriffskontrolle**  
Protokollierung von Zugriffen auf Anwendungen  
Nur berechtigte Mitarbeiter haben Zugriff auf Auftragsdatenverwaltung  
Physische Löschung von Datenträgern vor Wiederverwendung  
Zeitliche Begrenzung der Zugriffsmöglichkeiten  
Einsatz von Aktenvernichtern und Dienstleistern mit Datenschutz-Gütesiegel  
Separates Abfallmanagement für Produkte mit personenbezogene Daten  
Verschlossene Abfallbehälter im Außenbereich  
Sichere Aufbewahrung von Datenträgern
5. **Weitergabekontrolle**  
Auftragsdaten werden in einem separierten, zugriffsgeschützten Speicherbereich abgelegt  
E-Mail-Verschlüsselungen  
Dokumentation der Empfänger von Daten  
Vereinbarung von Löschrufen  
Festmontierte Plattenspeicher  
Gesonderter Verschluss vertraulicher Daten und Datenträgern
6. **Eingabekontrolle**  
Protokollierung der Eingabe, Änderung und Löschung von Daten  
Aufbewahrung von Dokumenten, von denen Daten in automatisierte Verarbeitungen übernommen worden sind  
Veränderungen an Daten werden protokolliert
7. **Auftragskontrolle**  
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten hinsichtlich Datensicherheit  
Schriftliche Weisungen an den Auftragnehmer durch Auftragsdatenverarbeitungsvertrag  
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags  
Formalisierte Auftragserteilung und eindeutige Vertragsgestaltung  
Verpflichtung unserer Geschäftspartner auf Vertraulichkeit
8. **Verfügbarkeitskontrolle**  
Rauchmeldeanlagen, Brandschutz  
Aufbewahrung von Datensicherungen an einem ausgelagerten Ort  
Tägliche Datensicherungen  
Geschützte und räumlich getrennte Serverstandorte
9. **Getrennte Verarbeitung**  
Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern  
Auftragsspezifische SQL-Datenbanken  
Logische Mandantentrennung  
Getrennte Ordnerstrukturen (Auftragsdatenverarbeitung)

Haben Sie weitere Fragen? Bitte wenden Sie sich an: [post@strohm-druck.de](mailto:post@strohm-druck.de)