

Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages.

**Standortdefinitionen:**

- Standort Eppelborn, Koßmannstrasse7, 66571 Eppelborn  
Nachfolgend als „Zentrale“ bezeichnet
  
- Standort Losheim, Prof.-Pirlet-Straße 27 – 29, 66679 Losheim am See, Rechenzentrum KÜS  
Nachfolgend als „RZ-KÜS“ bezeichnet
  
- Standort Saarwellingen, 66793 Saarwellingen, Rechenzentrum VSE  
Nachfolgend als „RZ-VSE“ bezeichnet
  
- Standort Saarbrücken, Am Felsbrunnen 15, 66119 Saarbrücken  
Nachfolgend als „RZ-SB“ bezeichnet
  
- Standort Wiesbach, Hauptstraße 1, 66571 Eppelborn  
Nachfolgend als „Landheim“ bezeichnet

<b>1. Pseudonymisierung</b>
Zentrale: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-KÜS: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-VSE: Keine Maßnahmen zur Pseudonymisierung von Daten
RZ-SB: Keine Maßnahmen zur Pseudonymisierung von Daten
Landheim: Keine Maßnahmen zur Pseudonymisierung von Daten

## **2. Verschlüsselung**

### Zentrale:

- Verschlüsselung von Datentransfers für externe Zugriffe der Mitarbeiter mit VPN
- Verschlüsselter Zugang zum E-Mail-Server mit SSL
- Verschlüsselter Fernwartungszugang zu Kunden über VPN
- Verschlüsselung des Mailverkehrs mit ausgewählten Empfängern
- Verschlüsselung von sensiblen E-Mail-Anhängen an alle Empfänger

### RZ-KÜS:

- Verschlüsselter Datentransfer zwischen RZ-KÜS und anderen Standorten mit VPN

### RZ-VSE:

- Verschlüsselter Zugang zum ERP-System mit SSL
- Verschlüsselter Datentransfer zwischen RZ-VSE und anderen Standorten mit VPN
- Verschlüsselte Datenablage mit Zugriff über SSL (Saar-Storage)

### RZ-SB:

- Verschlüsselter Datentransfer zwischen RZ-SB und anderen Standorten mit VPN

### Landheim:

- Verschlüsselung von Datentransfers für externe Zugriffe der Mitarbeiter mit VPN

## **3. Vertraulichkeit**

### Zentrale:

- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Sensible Bereiche wie z.B. Serverraum sind zusätzlich durch Fenstergitter abgesichert
- Zugang zum Serverraum nur für autorisierte Personen (elektronische Zugangskontrolle)
- Alarmanlage
- Individueller Login für alle Mitarbeiter beim Anmelden ans Unternehmensnetzwerk
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Kennwörter müssen regelmäßig geändert werden (180 Tage)
- Kennwortchronik wird erzwungen für 24 gespeicherte Kennwörter
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

### RZ-VSE:

- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

### RZ-KÜS:

- 24/7 Pförtner, Zugang mit Ausweiskarte mit Bild
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

**RZ-SB:**

- Begleiteter Zugang nach Anmeldung für autorisierte Mitarbeiter
- Individueller Login für alle Techniker mit Fernzugriff
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

**Landheim:**

- Personalisierte elektronische Zugangskontrolle mit zugeordneten Namen
- Videoüberwachung
- Individueller Login für alle Mitarbeiter beim Anmelden ans Unternehmensnetzwerk
- Kennwörter müssen Komplexitätsvoraussetzungen entsprechen
- Kennwörter müssen regelmäßig geändert werden (180 Tage)
- Kennwortchronik wird erzwungen für 24 gespeicherte Kennwörter
- Bedarfsgerechte Zugriffs- und Nutzungsrechte

#### **4. Integrität**

**Alle Standorte:**

- Erteilung von Weisungen in schriftlicher Form (Ticket-System)
- Festgelegte Personen bzgl. Empfang und Erteilung von Anweisungen
- Automatisierte Prüfung der relevanten Dateisysteme auf Fehler (Monitoring)
- Regelmäßige zentral gesteuerte und überwachte Updates der Betriebssysteme
- Regelmäßige zentral gesteuerte und überwachte Updates der genutzten Programme
- Zentral gesteuertes und überwachtes Viren- Malware- und Ransomware-Schutz

**RZ-VSE:**

- Systemseitige Protokollierung von Eingaben im ERP-System

#### **5. Verfügbarkeit**

**Zentrale:**

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Datensicherung auf direkt verfügbare Systeme zur schnellen Datenwiederherstellung im Verlustfall (Backup-to-Disk)
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Brandmeldeanlage
- Temperaturüberwachung sensibler Bereiche
- Feuchtigkeitssensoren, Wassereintruchsmelder
- Unterbrechungsfreie Stromversorgung für alle Systeme mit Datenhaltung
- Separater Stromkreis

**RZ-KÜS:**

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Zertifizierung nach DIN EN 50600 (Teil1 und 2)
- Löschanlage mit einem System zur Brandfrüherkennung
- Klimatisierung
- Redundante Stromversorgung
- 24/7 Objektüberwachung durch einen Sicherheitsdienst
- 24/7 Videoüberwachung des kompletten Geländes und der Gebäude

**RZ-VSE:**

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Redundante 10 kV Stromzuführung
- Redundante Notstromversorgung
- TIER 4 Elektrotechnikstandards
- Löschgasanlage
- Schaltbare PDUs
- Klimatisierung
- Redundante Stromversorgung

**RZ-SB:**

- Redundante Systeme mit entsprechender Ausfallsicherheit auf mehreren Ebenen
- Duplizierung der Datensicherung auf getrennt gelagerte Medien
- Klimatisierung
- Zertifizierung nach ISO/IEC 27001
- Videoüberwachung und Aufzeichnung im Gebäude und auf der Außenanlage
- Monitoring der kompletten Infrastruktur
- redundante Anbindung an Internet-Backbones
- unterbrechungsfreie Stromversorgung mit redundanter Gebäudezuführung
- Leckage Warnanlage zum Schutz vor Wassereintrüben

**Landheim:**

- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

## **6. Belastbarkeit der Systeme**

### Zentrale:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Zentral verwaltete Anti-Ransom-Lösung
- Unterbrechungsfreie Stromversorgung für alle Systeme mit Datenhaltung
- Separater Stromkreis für Serverraum
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung bei Bedarf
- Monitoring aller relevanten Ressourcen
- Einsatz von RAID-Systemen
- Redundante Virtualisierungshost-Systeme

### RZ-KÜS:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

### RZ-VSE:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

### RZ-SB:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Unterbrechungsfreie Stromversorgung
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- Klimatisierung
- Redundante Virtualisierungshost-Systeme

### Landheim:

- Firewallsystem mit individuellem Regelwerk
- Zentral verwaltete Anti-Virus-Software
- Überwachung aller Systeme bzgl. Auslastung und Nutzung
- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

**7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall**

Zentrale:

- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-VSE:

- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-SB:

- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

RZ-KÜS:

- Regelmäßige Tests der Datensicherung durch Rücksicherung und Validierung
- Aufbewahrung der Sicherungsmedien an verschiedenen physisch getrennten Standorten
- Instant-Recovery zur sofortigen Wiederherstellung der Verfügbarkeit direkt aus dem Backup-System

Landheim:

- An diesem Standort befinden sich keine Server oder andere Systeme mit aktiver Datenspeicherung

**8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**

Alle Standorte:

- Datenschutz-Management-System (PDCA-Modell)
  - o Es wurde ein externer betrieblicher Datenschutzbeauftragter bestellt.
  - o Regelmäßige Abstimmung mit dem Datenschutzbeauftragten.
  - o Mitarbeiter werden auf die Vertraulichkeit verpflichtet.
  - o Die Mitarbeiter werden mindestens einmal jährlich auf den Datenschutz hin sensibilisiert.
  - o Verzeichnis der Verarbeitungstätigkeiten wird fortlaufend aktualisiert.
  - o Datenschutz-Folgenabschätzungen (DSFA) werden bei Bedarf durchgeführt.
  - o Prozess zur Wahrnehmung von Betroffenenrechten etabliert.
  - o Prozess zur Meldung von Datenschutzverstößen etabliert.
  - o Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen durch entsprechende Tasks und Checklisten im ERP-System
  - o Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenschutzverstöße.

○ Vertragsmanagement (Auftragsverarbeiter)

- Die Standorte RZ-KÜS, RZ-VSE und RZ-SB werden vorlaufend ISO 27001 zertifiziert
- Regelmäßige Überprüfung der Aktualisierung der eingesetzten Firewalls
- Regelmäßige Überprüfung der Aktualisierung der eingesetzten Spamfilter
- Regelmäßige Überprüfung der Aktualisierung eingesetzter Virens Scanner
- Auswahl der Auftragsverarbeiter unter Sorgfaltsgesichtspunkten
- Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragsverarbeiter bei Vorliegen einer Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter