# Technische und organisatorische Maßnahmen des Auftragnehmers

Die HETTENBACH GMBH & CO KG stellt über die folgenden Maßnahmen sicher, dass dem jeweiligen Schutzbedarf bei der Verarbeitung personenbezogener Daten entsprochen wird.

## 1. Zutrittskontrolle

Ein unbefugter Zutritt wird verhindert durch Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Schlüsselkonzept mit Zutrittsberechtigung / Schlüsselvergabe protokolliert
- Zutrittsregelung für Serverraum und Personalbereich nur für autorisierte Personen

## 2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme wird verhindert durch entsprechende Benutzeridentifikation und Authentifizierung:

- Benutzername / individualisiertes Passwortverfahren
- Verschlüsselung von mobilen Datenträgern und mobilen Geräten

## 3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen werden durch ein detailliertes Berechtigungskonzept mit Protokollierung der Zugriffsrechte verhindert.:

- Regelung der Berechtigungen über Administrationskonzept
- Differenzierte Berechtigungen (Profile) nach Abteilungen und Tätigkeiten
- Externer Datenverkehr über verschlüsselte Zugangsverbindungen (VPN)
- Datenschutzgerechte Aktenentsorgung

## 4. Weitergabekontrolle

Dem Schutzbedarf bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger wird entsprochen durch:

- Verschlüsselung / Ausgabekontrolle manueller Datenträger
- Tunnelverbindung (VPN = Virtual Private Network)
- Elektronische Übermittlung über passwortgeschützten FTP-Server

## 5. Eingabekontrolle

Zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, verwenden wir:

- Protokollauswertungssysteme über Nutzeranmeldung
- Professional ERP-System: Änderungsprotokoll

## 6. Auftragskontrolle

Bei der Vergabe von Aufträgen zur Datenverarbeitung an Dritte stellen wir grundsätzliche folgende Voraussetzungen sicher:

- Schulung der Mitarbeiter in Bezug auf Umgang mit personenbezogenen Daten
- Verpflichtung der Mitarbeiter auf die Einhaltung des Datenschutz
- Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
- Kontrolle der Vertragsausführung

## 7. Verfügbarkeitskontrolle

Die Nutzbarkeit der Daten stellen wir durch folgende Verfügbarkeitsmaßnahmen sicher:

- Backup-Verfahren
- Storage (Datenspeicher) mit RAID-Verfahren
- Redundante, unterbrechungsfreie Stromversorgung (USV)
- Virenschutz / Firewall
- Redundante Server mit virtualisierten Systemen
- Rechenzentrum kann gemäß Notfallplan nach Prioritäten hochgefahren werden
- Wartungs- und Supportverträge mit externen Dienstleistern (Server, Storage, Switch, Autoloader,..)

## 8. Trennungskontrolle

Falls wir Daten zu unterschiedlichen Zwecken erheben, werden diese getrennt verarbeitet. wurden, sind auch getrennt zu verarbeiten. Dies wird sichergestellt durch:

- Zweckbindung
- Getrennte physische / elektronische Speicherorte besonderer Kategorien von Daten

## 9. Datenträgerkontrolle

Um Daten und Datenträger vor unbefugtem Lesen, Kopieren, Verändern oder Löschen zu schützen, wurde folgendes realisiert:

- Zentraler Storage im Rechenzentrum
- Backups werden auf Backup-Storage und Bänder geschrieben
- Bänder werden außerhalb des Rechenzentrum sicher aufbewahrt

Stand: 24.10.2024