

# Technische und organisatorische Maßnahmen

## *Technical and organizational measures*

nach Art. 32 DSGVO | *in accordance with Art. 32 of the GDPR*

der | of

**HÖRMANN Intralogistics Solutions GmbH**

Gneisenaustraße 15

80992 München | *Munich*

### 1 Transparenz | *Transparency*

- ◆ Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. ***Documentation of the nature, scope, circumstances, and purposes of the processing.***
- ◆ Dokumentation der Mandanten und zugehörigen Datenbereiche. ***Documentation of clients and associated data areas.***
- ◆ Dokumentation von Auftrags- und Unterauftragsverhältnissen. ***Documentation of contract and subcontract relationships.***
- ◆ Bereitstellung der erforderlichen Dokumentationen auf Antrag der betroffenen Person. ***Providing the necessary documentation upon request of the data subject.***
- ◆ Dokumentation der Löschrufen. ***Documentation of deletion periods.***
- ◆ Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten (z. B. online oder als Aushang) als Datenschutzerklärung. ***Publication of information regarding the processing of personal data (e.g., online or as a notice) as a privacy statement.***

### 2 Zweckbindung | *Purpose limitation*

- ◆ Darstellung der Zwecke im Verzeichnis von Verarbeitungstätigkeiten. ***Representation of purposes in the record of processing activities.***
- ◆ Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten. ***Issuance of a written service instruction for the processing of personal data.***
- ◆ Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DSGVO. ***Obligation of employees to comply with the requirements of the GDPR.***
- ◆ Entgegennehmen ausschließlich schriftlicher Weisungen (jedenfalls in Textform, z.B. E-Mail) nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers. ***Receipt of instructions exclusively in writing only (at least in written form, e.g., email) from authorized employees of the controller or client.***

### 3 Datenminimierung | *Data minimization*

- ◆ Festlegung verbindlicher Löschrufen. ***Establishment of binding deletion deadlines.***
- ◆ Festlegung automatisierter Löschrufen. ***Establishment of automated deletion cycles.***

---

**Technische und organisatorische Maßnahmen | Technical and organizational measures****4 Richtigkeit | Accuracy**

- ◆ Zertifikatsbasierte Authentifizierung der Datenquelle Entra-ID (AAD). **Certificate-based authentication of the data source Entra-ID (AAD).**
- ◆ Beantragung einer Berichtigung durch elektronische Antragstellung. **Application for correction through electronic application submission.**
- ◆ Einrichtung eines Verfahrens zur Berichtigung von Daten auf Antrag per E-Mail. **Establishment of a procedure for data correction upon request via email.**

**5 Vertraulichkeit | Confidentiality**

- ◆ **Clean Desk policy.**
- ◆ Zugang nur mit Parkkarte. **Access only with parking card.**
- ◆ Parkplatzschranke. **Parking barrier.**
- ◆ Technikkeller mit Schlüsselausgabeliste. **Technical room with key issuance list.**
- ◆ Archivkeller mit Zugriffsbeschränkung. **Archive cellar with access restriction.**
- ◆ Sichere Behältnisse bei physischem Transport. **Secure containers for physical transport.**
- ◆ Alarmanlage im Gebäude. **Alarm system in the building.**
- ◆ Sicherheitsschlösser. **Security locks.**
- ◆ Personenkontrolle anhand des Besucherformulars. **Personnel control based on the visitor form.**
- ◆ Auf Datenschutz verpflichtetes Reinigungspersonal. **Privacy-committed cleaning staff.**
- ◆ Unterteilung in Sicherheitszonen. **Division into security zones.**
- ◆ Schlüsselregelung. **Key control arrangement.**
- ◆ Schließsystem mit Transponder. **Locking system with transponder.**
- ◆ Zugangskontrollsystem. **Access control system.**
- ◆ Einbruchhemmende Türen. **Burglar-resistant doors.**
- ◆ Festgelegte Reinigungszeiten. **Established cleaning schedules.**
- ◆ Manuelles Schließsystem. **Manual locking system.**
- ◆ Zugangsbeschränkung nach Endgerät. **Access restriction by device.**
- ◆ Benutzerkonto für jeden Mitarbeiter. **User account for each employee.**
- ◆ Arbeiten mit individuellen Benutzerkennungen. **Use of individual user IDs.**
- ◆ Regelmäßige Passwortwechsel. **Regular password changes.**
- ◆ Authentifikation mit Passwort. **Authentication with password.**
- ◆ Automatische Sperrung. **Automatic locking.**
- ◆ Aufteilung der Administratorrechte unter verschiedenen Personen. **Division of administrator rights among different individuals.**
- ◆ Zertifiziertes Löschen von Datenträgern. **Certified erasure of data carriers.**
- ◆ Sperren der Bootkonfiguration (BIOS, UEFI). **Locking of boot configuration (BIOS, UEFI).**
- ◆ Kontensperrung nach mehrmaliger Falscheingabe des Passworts. **Account lockout after multiple incorrect password entries.**
- ◆ Keine Adminrechte außerhalb der internen IT. **No admin rights outside internal IT.**
- ◆ Differenzierung administrativer Aufgaben. **Differentiation of administrative tasks.**
- ◆ Physikalisch getrennte Speicherung und Verarbeitung. **Physically separated storage and processing.**

---

**Technische und organisatorische Maßnahmen | Technical and organizational measures**

- ◆ Datenträgervernichtung nach DIN 66399. **Data carrier destruction according to DIN 66399.**
- ◆ Trennung von Produktiv- und Testsystem. **Separation of productive and test systems.**
- ◆ Dem Zweck angemessene Passworrichtlinien. **Password policies appropriate to the purpose.**
- ◆ Authentifikation über Verzeichnisdienste. **Authentication via directory services.**
- ◆ Regelungen beim Ausscheiden von Mitarbeitern. **Provisions for employees leaving the company.**
- ◆ Sicheres Löschen einzelner Dateien. **Secure deletion of individual files.**
- ◆ Beaufsichtigung von Wartungstätigkeiten. **Supervision of maintenance activities.**
- ◆ Nach Verarbeitungszweck differenziertes Berechtigungskonzept. **Authorization concept differentiated by processing purpose.**

**6 Pseudonymisierung | Pseudonymization**

- ◆ Datenschutz durch Technikgestaltung. **Data protection by design.**
- ◆ Vornahme datenschutzfreundlicher Voreinstellungen. **Data protection by default.**
- ◆ Datenträgerverschlüsselung. **Data carrier encryption.**
- ◆ Transportverschlüsselte Datenübertragung. **Transport encrypted data transmission.**
- ◆ Durchgängige Transportverschlüsselung bei der E-Mail-Übertragung. **Consistent transport encryption in email transmission.**
- ◆ Datenkommunikation über VPN-Tunnel. **Data communication via VPN tunnel.**
- ◆ Dateiverschlüsselung. **File encryption.**
- ◆ Verschlüsselung der Internetpräsenz. **Encryption of the internet presence.**
- ◆ Inhaltsverschlüsselte Datenübertragung. **Content-encrypted data transmission.**
- ◆ Verschlüsselung von mobilen Datenträgern. **Encryption of mobile storage devices.**

**7 Integrität | Integrity**

- ◆ Einsatz von Virenschutzlösungen. **Use of antivirus solutions.**
- ◆ **Intrusion Detection System.**
- ◆ **Packet Filter Firewall.**
- ◆ Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste. **Automated update processes for operating systems, applications, and services.**
- ◆ Plausibilitätskontrollen bei der Datenverarbeitung. **Plausibility checks in data processing.**
- ◆ Regelung zum Umgang mit mobilen Datenträgern. **Guidelines for handling mobile storage devices.**
- ◆ Anti Spam Filter für geschäftliche E-Mails. **Anti-Spam filter for business emails.**
- ◆ Differenzierte Berechtigungen für Datenobjekte. **Differentiated permissions for data objects.**

---

**Technische und organisatorische Maßnahmen | Technical and organizational measures****8 Verfügbarkeit | Availability**

- ◆ Sicherungs- und Wiederherstellungs- konzept. **Backup and Recovery Concept.**
- ◆ Aufbewahrung von Datenträgern in gegen Elementarschäden gesicherten Behältnissen. **Storage of data carriers in containers secured against elemental damage.**
- ◆ Festgelegte Zuständigkeiten für die Datensicherung. **Designated responsibilities for data backup.**
- ◆ Notfallplan zur Wiederinbetriebnahme von Servern und Diensten. **Emergency plan for the restoration of servers and services.**
- ◆ Notfallplan bei Kompromittierung. **Emergency plan in case of compromise.**
- ◆ Redundante IT-Systeme. **Redundant IT systems.**
- ◆ Automatisches Benachrichtigungssystem bei Ausfall. **Automated notification system in case of failure.**
- ◆ Automatisiertes Anfertigen von Datensicherungen (Backup). **Automated data backup (Backup).**
- ◆ Aufbewahrung der Datensicherung in einem anderen Brandabschnitt. **Storage of backups in a different fire compartment.**
- ◆ Regelmäßiger Test der Datenwiederherstellung. **Regular testing of data recovery.**
- ◆ Datenträgerspiegelung (RAID). **Data mirroring (RAID).**
- ◆ Notfallplan bei Datenverlust. **Emergency plan for data loss.**
- ◆ Virtualisierte Infrastruktur. **Virtualized infrastructure.**

**9 Belastbarkeit | Resilience**

- ◆ Unterbrechungsfreie Stromversorgung. **Uninterruptible Power Supply (UPS).**
- ◆ Klimaanlage in Serverräumen. **Air conditioning in server rooms.**
- ◆ Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen. **Climate monitoring (room temperature, humidity) in server rooms.**
- ◆ Feuchtigkeitssensoren im Archiv. **Humidity sensors in the archive.**
- ◆ Überspannungsschutz. **Surge protection.**
- ◆ Feuer- und Rauchmeldeanlagen. **Fire and smoke detection systems.**
- ◆ Feuerlöscher. **Fire extinguishers.**
- ◆ IT-Komponenten verfügen über erforderliche Leistungsfähigkeit. **IT components have the necessary performance capabilities.**
- ◆ Eignung der Räumlichkeiten / des Baus. **Suitability of premises/building.**

---

**Technische und organisatorische Maßnahmen | Technical and organizational measures****10 Rechenschaftspflicht | Accountability**

- ◆ Führen eines Verzeichnisses von Verarbeitungstätigkeiten. ***Maintaining a record of processing activities.***
- ◆ Dokumentation über vorhandene IT- Infrastruktur. ***Documentation of the existing IT infrastructure.***
- ◆ Dokumentation der getroffenen Sicherheitsmaßnahmen. ***Documentation of the implemented security measures.***
- ◆ Protokollierung der Anmeldevorgänge. ***Logging of login processes.***
- ◆ Protokollierung gescheiterter Zugriffsversuche. ***Logging of failed access attempts.***
- ◆ Automatisierte Auswertung der Protokolldaten. ***Automated analysis of log data.***
- ◆ Protokollierung von Löschvorgängen. ***Logging of deletion processes.***
- ◆ Protokollierung von Administratorenaktivitäten. ***Logging of administrator activities.***
- ◆ Stichprobenartige Überprüfung der Wirksamkeit bestimmter Maßnahmen. ***Random checks on the effectiveness of certain measures.***
- ◆ Bestellung eine(r/s) Datenschutzbeauftragten. ***Appointment of a Data Protection Officer (DPO).***
- ◆ Dokumentation über eingesetzte Programme und Anwendungen. ***Documentation of deployed programs and applications.***
- ◆ Protokollierung der Datenzugriffe in der Cloud. ***Logging of data accesses in the cloud.***
- ◆ Sicherung der Protokolldaten gegen Veränderung und Verlust. ***Securing log data against alteration and loss."***
- ◆ Protokollierung der Datenträgervernichtung. ***Logging of data destruction processes.***
- ◆ Benutzerkennungsbezogene Protokollierung bei Anmeldung. ***User-specific logging during login.***
- ◆ Arbeitssicherheitsunterweisungen Büro und Baustelle. ***Occupational safety training for office and construction site.***
- ◆ Brandschutzschulungen für betriebliche Ersthelfer. ***Fire protection training for company first aiders.***
- ◆ externe Ersthelferkurse. ***External first aid courses.***
- ◆ Protokollierung der sicheren Löschungen von Datenträgern. ***Logging of secure deletions of data carriers.***