Stand: 01.11.2023

Erfassung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO der driveMybox logistics GmbH

Maßnahmengruppe	Maßnahmen
Maßnahmen zur Sicherstellung der Vertraulichkeit *Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen)*	• Aufteilung des Betriebsgebäudes in differenzierte Zutrittsbereiche mit Zutrittskontrolle • mechanische Schließsysteme – Sicherheitsschlösser • Schlüsselverwaltung / Dokumentation der Schlüsselvergabe • elektronisches Zutrittssystem (RFID) mit Berechtigungsverwaltung • Zutrittsregelung für betriebsfremde Personen
Zugangskontrolle (keine unbefugte Systemnutzung)	• Passwortrichtlinie zur Plattform – Mindestlänge und Zusammensetzung vorgeschrieben – 8 Zeichen; regelmäßiger Wechsel von Passwörtern ohne Wiederholungen nach 77 Wochen • Protokollierung von Logins / Loginversuchen (max. 7 Fehlversuche) • Benutzerrichtlinie (Identifikation und Authentifizierung von Benutzern mit Benutzername und Passwort) • sicheres Aufbewahren von Administrationspasswörtern • Automatische Bildschirmsperren • Auswertung von Zugriffsprotokollen hinsichtlich Unregelmäßigkeiten • Einsatz von Anti-viren/phishing-software • Verwendung von SSL und SSH Verbindungen für externe Zugänge • verschlüsselte Datenablage auf mobilen IT-Systemen • regelmäßige Sicherheitsupdates von Programmen und Systemen • Netzwerksegmentierung • Login-Sperre für 30 Minuten nach 7 Fehlersuchen innerhalb von 30 Minuten
Zugriffskontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im System)	• Berechtigungskonzept für Benutzerkonten • need-to-know-Prinzip über disponierbare Benutzerkonten und Rollenmodell • regelmäßige Kontrolle der Zugriffsberechtigungen (ausgeschiedene Mitarbeiter!) • eingeschränkte Anzahl und Regelungen von Administratorenkonten • Überwachung und Protokollierung von Zugriffen • Verschlüsselung mobiler Endgeräte

Maßnahmengruppe	Maßnahmen
	• ordnungsgemäße Vernichtung von Datenträgern
Zwecktrennungsgebot (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)	• logische Datentrennung • Trennung von Produktiv- und Entwicklungs- / Testsystemen
Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)	• Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;
Maßnahmen zur Sicherstellung der Integrität *Weitergabekontrolle (kein unbefugtes Lesen, Kopieren oder Entfernen bei elektronischer Übertragung oder Transport)*	• Verwendung von SSL und SSH Verbindungen für externe Zugänge • Einsatz sicherer Cloudlösung zum Datentransfer • Verbot des Einsatzes privater Datenträger • sicheres Löschen / Entsorgen von Datenträgern (Löschroutinen bzw. zertifizierter Entsorger) • verschlüsselte Versendung von Daten mit sensitivem Inhalt
Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt wurden)	• Protokollierung von Eingaben – mit Nutzerkennung • Einsatz von Berechtigungskonzepten • Verwendung eines Dokumentenmanagements • Transaktionskontrollen • Schadsoftwarekontrolle • Netzwerkdokumentation ist vorhanden
Maßnahmen zur Sicherstellung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit *Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)*	• Backup-Strategie vorhanden (online / offline; on-site / off-site) • Backup täglich / wöchentlich • sichere Aufbewahrung von Backup-Medien • Verwendung unterbrechungsfreie Stromversorgung (USV) • Überspannungsschutz vorhanden • Einsatz von Brandschutzsystemen • klimatisierte Räume / Temperaturüberwachung • Meldewege und Notfallpläne sind etabliert • Intrusion-Detection / Prevention-Systeme werden eingesetzt
Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung *Datenschutzmanagement*	• regelmäßige Audits • Kontrolle durch externen Datenschutzbeauftragten
Incident-Response-Management	• Dokumentierte Ab-/ Aufarbeitung von Informationssicherheitsvorfällen

Maßnahmengruppe	Maßnahmen
	• Aufarbeiten von Informationssicherheitsvorfällen nach eigenem Verfahren
Datenschutzfreundliche Voreinstellungen	• Umsetzung Passwortrichtlinie • Hardware-Verschlüsselung mobiler Endgeräte
Auftragskontrolle	• eindeutige Vertragsgestaltung
	• formalisiertes Auftragsmanagement
	• kritische Auswahl der Dienstleister
	• Vorabüberzeugungspflicht
	• regelmäßige Kontrollen