Anlage zum Auftragsverarbeitungsvertrag - technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Die erforderlichen Maßnahmen werden gemäß den Vorgaben wie folgt festgeschrieben:

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Betriebsgelände und Büros:
- Sicherheitsschlösser
- elektrischer Toröffner
- Alarmanlagen

LKW, Datenvernichtung vor Ort:
- Festlegung der zutrittsberechtigten Mitarbeiter
- Definition der Zutrittsberechtigten des Auftraggebers bei Auftragsannahme, schriftliche Dokumentation in Auftragsbestätigung oder Anlage 2 zutrittsberechtigte Personen
- Kontrolle vor Ort durch die Mitarbeiter der sicher-vernichtet.de
- fester geschlossener Kofferaufbau
- Videoüberwachung und -aufzeichnung im Innenraum/Einfüllschacht der Vernichtungsanlage

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

Betriebsgelände und Büros:
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Verschlüsselung von Datenträgern
- Berechtigungskonzept
- Einsatz einer Firewall

LKW, Datenvernichtung vor Ort:
- Bedienung der Datenverarbeitungsanlage nur durch eingewiesene und berechtigte Mitarbeiter
- Zutrittskontrolle am Fahrzeug durch Mitarbeiter der sicher-vernichtet.de
- Verbotsschilder: Verbot des Zutritts für Unbefugte zur Datenverarbeitungsanlage
- Bedienung der Datenvernichtungsanlage nur durch Schließsystem möglich
- passwortgeschütztes System zur Videoüberwachung

Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Betriebsgelände und Büros:
- Berechtigungskonzept
- Bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Verschlüsselung von Datenträgern

LKW, Datenvernichtung vor Ort:

• Ausschließlich weisungsgebundene Datenvernichtung am Gelände des Auftraggebers

Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Betriebsgelände und Büros:
• Berechtigungskonzept
• Festlegung von Datenbankrechten

LKW, Datenvernichtung vor Ort:
• Ausschließlich weisungsgebundene Datenvernichtung am Gelände des Auftraggebers

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Das bedeutet, dass die Daten vollständig und unverändert sind.

Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Betriebsgelände und Büros:
• E-Mail-Verschlüsselung
• Verschlüsselung von Datenträgern

LKW, Datenvernichtung vor Ort:
• Legitimation der Berechtigten
• Transport von unvernichteten Datenträgern zum Fahrzeug nur in geeigneten verschlossenen Behältern
• Definition der Bereiche, in denen sich Datenträger befinden dürfen
• Festlegung der berechtigten Personen, die Datenträger aus diesen Bereichen entfernen dürfen
• Nachkontrolle nach der Vernichtung ob Datenträger vollständig vernichtet wurden, kein Verbleib von unvernichteten Datenträgern am Fahrzeug

Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Betriebsgelände und Büros:
• Protokollierung der Eingabe, Änderung und Löschung von Daten
• Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

LKW, Datenvernichtung vor Ort:
• Ausschließlich weisungsgebundene Datenvernichtung am Gelände des Auftraggebers

Verfügbarkeit und Belastbarkeit

Die Verfügbarkeit von Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Betriebsgelände und Büros:
• Backup- und Recovery-Konzept

- unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Serverräume nicht unter sanitären Anlagen

LKW, Datenvernichtung vor Ort:
- Ausschließlich weisungsgebundene Datenvernichtung am Gelände des Auftraggebers

Rasche Wiederherstellbarkeit

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Betriebsgelände und Büros:
- Backup- und Recovery-Konzept
- unterbrechungsfreie Stromversorgung (USV)

LKW, Datenvernichtung vor Ort:
- Ausschließlich weisungsgebundene Datenvernichtung am Gelände des Auftraggebers

Verfahren zur regelmäßigen Überprüfung und Bewertung

Datenschutz-Management

Eine Datenschutzorganisation muss im Unternehmen etabliert und eine Datenschutz-Management-System aufgebaut und gepflegt werden. In der sicher-vernichtet.de GmbH ist die Datenschutzorganisation mit Zuweisung aller Verantwortlichkeiten etabliert. Ein Datenschutzbeauftragter ist benannt. Das Datenschutz-Management-System mit allen benötigten Dokumentationen zur Nachweispflicht ist erstellt und wird permanent gepflegt.

Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Betriebsgelände und Büros (als Auftraggeber):
- Eindeutige Vertragsgestaltung mit externen Dienstleistern
- Formalisiertes Auftragsmanagement
- Regelung der Rechte und Pflichten des Auftragnehmers und des Auftraggebers
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht
- Nachkontrollen

LKW, Datenvernichtung vor Ort (als Auftragnehmer):
- schriftliche Entsorgungsverträge zur mobilen Datenträgervernichtung
- Regelung der technischen und organisatorischen Maßnahmen
- Regelung der Rechte und Pflichten des Auftragnehmers und des Auftraggebers
- Kontrolle vor Ort durch beide Parteien
- Überprüfung der ordnungsgemäßen Datenvernichtung jederzeit vor Ort möglich

Stand: 10.02.2023