# Technische und organisatorische Maßnahmen zur Datensicherheit

Bei der Auerswald GmbH sind nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i. S. d. Art. 32 DSGVO getroffen worden:

## 1. Vertraulichkeit

### 1.1. Zutrittskontrolle

Die Auerswald GmbH ist auf zwei Standorte in 38162 Cremlingen verteilt:

- Standort „Hordorfer Straße 36“:
  Produktion, Reparatur, Einkauf, Versand sowie das firmeneigene Schulungscenter
- Standort „Vor den Grashöfen 1“:
  Entwicklung, Buchhaltung, Personalabteilung, Vertrieb, Marketing und Produktmanagement

**Zutrittsregelung für Mitarbeitende**

Beide Gebäude sind rund um die Uhr verschlossen. Zutritt erhalten ausschließlich Beschäftigte der Auerswald GmbH über ein elektronisches Schließsystem, das von der IT- und Personalabteilung verwaltet wird. Die Ausgabe und Verwaltung von Transpondern erfolgen nach einem dokumentierten Prozess sowohl beim Eintritt als auch beim Austritt eines Beschäftigten. Zutrittsrechte werden nach dem Grundsatz der Erforderlichkeit („Need-to-Access“) vergeben. Beschäftigte erhalten nur Zugang zu den Bereichen, die für ihre Tätigkeit erforderlich sind.

**Zutrittsregelung für Besucher**

- Standort „Hordorfer Straße 36“:

  Besucher erhalten Zutritt nur nach Türöffnung durch den Empfang oder eine berechtigte Person. Der Empfang hat Sichtkontakt zum Eingangsbereich und stellt sicher, dass sich jeder Besucher anmeldet. Gespräche mit externen Personen finden ausschließlich in vorgesehenen Besprechungsräumen statt.

  Teilnehmer von Schulungen der Auerswald Academy dürfen sich nur im ausgewiesenen Bereich des Schulungszentrums bewegen. Der Zugang zu Büro- und Produktionsbereichen ist durch das Transpondersystem gesichert und nicht

gestattet. Ausnahmen hiervon bilden Werksbesichtigungen, diese sind nach vorheriger Anmeldung und Dokumentation möglich.

- Standort „Vor den Grashöfen 1“:

  Dieser Standort ist grundsätzlich nicht für Besucher vorgesehen. In Ausnahmefällen ist ein Besuch nach vorheriger telefonischer Anmeldung und persönlicher Abholung am Eingang möglich. Der Besucher muss sich in das Besucherbuch eintragen.

**Sicherheitsmaßnahmen**

Außerhalb der regulären Arbeitszeiten ist der Zutritt zu den Gebäuden neben dem Transponder nur mit einem individuellen, mitarbeiterbezogenen Code möglich. Zudem ist die Zufahrt zum Firmengelände in der Hordorfer Straße durch ein elektronisch gesteuertes Tor gesichert, das ausschließlich per Transponder geöffnet werden kann. Die Produktions-, Reparatur-, Versand- und Lagerbereiche am Standort Hordorfer Straße sind zusätzlich durch eine Alarmanlage geschützt. Alle Beschäftigten sind im Umgang mit der Anlage geschult.

## 1.2. Zugangskontrolle

Zugriffe auf IT-Systeme sind nur mit einer gültigen Benutzerberechtigung möglich. Die Vergabe erfolgt ausschließlich auf Antrag durch die jeweilige Führungskraft oder die Personalabteilung und wird durch Administratoren umgesetzt.

**Authentifizierung**

Jede Benutzerkennung ist eindeutig. Initialpasswörter müssen nach der ersten Anmeldung geändert werden. Die Passwortrichtlinie der Auerswald GmbH sieht Folgendes vor:

- Mindestlänge: 12 Zeichen
- Verwendung von Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen
- Sperrung nach dreimaliger Falscheingabe
- Passwörter werden verschlüsselt gespeichert. Systeme erzwingen eine automatische Bildschirmsperre nach 5 Minuten Inaktivität.

**Netzwerksicherheit**

Remote-Zugriffe erfolgen ausschließlich über verschlüsselte VPN-Verbindungen. Alle Server- und Clientsysteme verfügen über aktuelle Virenschutzsoftware und sind durch Firewalls abgesichert. Ein Intrusion-Prevention-System erkennt und verhindert unbefugte Zugriffsversuche.

Alle Systeme werden regelmäßig mit Sicherheitsupdates und Patches versorgt.

### 1.3. Zugriffskontrolle

Berechtigungen für IT-Systeme und Anwendungen werden ausschließlich durch Administratoren eingerichtet und nach dem Need-to-Know-Prinzip vergeben. Es existiert ein rollenbasiertes Berechtigungskonzept, das sicherstellt, dass Beschäftigte nur auf Daten zugreifen können, die sie für ihre jeweilige Aufgabe benötigen. Projektbezogene Rechte können temporär vergeben und widerrufen werden.

Die Vernichtung von Datenträgern und Papier erfolgt durch einen zertifizierten Dienstleister nach DIN 66399. Beschäftigte sind verpflichtet, personenbezogene oder vertrauliche Daten ausschließlich in dafür vorgesehenen Sicherheitsbehältern zu entsorgen.

Die Installation nicht genehmigter Software auf IT-Systemen ist untersagt.

### 1.4. Trennung von Daten

Alle von Auerswald GmbH für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

### 1.5. Pseudonymisierung und Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungs-systeme im Einsatz.

## 2. Integrität

### 2.1. Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die von der Auerswald GmbH im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

### 2.2. Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden der Auerswald GmbH erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem

Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten nur verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei der Auerswald GmbH im Zusammenhang mit Kundenprojekten untersagt.

Mitarbeiter bei der Auerswald GmbH werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

## 3. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen der Auerswald GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.

Das Einspielen von Backups wird regelmäßig getestet.

Die Auerswald GmbH verfügt an beiden Standorten über je einen Serverraum. Beide Serverräume sind klimatisiert, liegen oberhalb der Wassergrenze und verfügen über eine unterbrechungsfreie Stromversorgung (USV) sowie Brandmeldeanlagen mit geeigneten Löschanlagen. Darüber hinaus übernimmt bei längeren Unterbrechungen ein Dieselaggregat die Stromversorgung des am Standort „Vor den Grashöfen 1“ befindlichen Haupt-Serverraums.

Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Ein Notfall- und Wiederanlaufplan ist dokumentiert und wird regelmäßig getestet.

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei der Auerswald GmbH ist ein Datenschutzmanagement implementiert. Dieser beinhaltet sowohl einen Krisenreaktionsplan bei Datenpannen als auch einen Prozess zur Meldung von Datenschutzverstößen an die zuständige Aufsichtsbehörde.

Die Richtlinien im Rahmen des Datenschutzmanagement werden jährlich im Hinblick auf ihre Wirksamkeit durch das Datenschutz- und Informationssicherheits-Team evaluiert und angepasst.

Es ist sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem Datenschutzbeauftragten oder stellvertretend dem Datenschutz- und Informationssicherheits-Team gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet

werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.

### 4.1. Auftragskontrolle

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich innerhalb der Europäischen Union.

Ein externer Datenschutzbeauftragter ist für die Auerswald GmbH benannt. Vor der Einbindung externer Dienstleister wird ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO abgeschlossen. Die Dienstleister werden vorab geprüft und regelmäßig kontrolliert.

### 4.2. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bereits bei der Entwicklung der Softwarelösungen der Auerswald GmbH werden die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt. Beispielsweise kann eine Multifaktorauthentifizierung aktiviert und der Zugriff über ein differenziertes Rollen- und Rechtekonzept gesteuert werden. Ein manipulationssicherer Audit-Trail dokumentiert sämtliche Änderungen an personenbezogenen Daten und Berechtigungen nachvollziehbar.

Zugriffsrechte werden nach dem Prinzip der Datenminimierung vergeben.