Datenschutz und Datensicherheit bei der KnowHow! AG
Version 3.0 – März 2026

1. Allgemeines

KnowHow! AG trifft als Auftragsverarbeiter gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten.

Dabei werden insbesondere berücksichtigt:

- Stand der Technik
- Implementierungskosten
- Art, Umfang und Zweck der Verarbeitung
- unterschiedliche Eintrittswahrscheinlichkeit und Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen.

Die Maßnahmen dienen insbesondere der Gewährleistung von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit der Systeme und Dienste
- Wiederherstellbarkeit von Daten
- regelmäßiger Überprüfung und Bewertung der Sicherheitsmaßnahmen.

2. Organisation des Datenschutzes

Datenschutzorganisation

- Bestellung eines Datenschutzbeauftragten gemäß Art. 37 DSGVO
- Beratung und Kontrolle durch den Datenschutzbeauftragten
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO

Auftragsverarbeitung

- Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO
- sorgfältige Auswahl und Kontrolle eingesetzter Subdienstleister
- vertragliche Verpflichtung auf Datenschutz und Vertraulichkeit

Mitarbeiter

- Verpflichtung aller Mitarbeitenden auf Vertraulichkeit
- regelmäßige Schulungen zu Datenschutz und Informationssicherheit

- interne Richtlinien zur Nutzung von IT-Systemen

3. Technische und organisatorische Maßnahmen

3.1 Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen:

- Zugang zu Betriebsräumen nur für autorisierte Personen
- gesicherter Serverraum
- Besucherregelungen mit Anmeldung und Begleitung
- geregelte Schlüsselverwaltung

3.2 Zugangskontrolle

Verhinderung der unbefugten Nutzung von IT-Systemen:

- Benutzerkonten mit individuellen Kennungen
- Passwortschutz und Authentifizierungsverfahren
- automatische Bildschirmsperren bei Inaktivität
- regelmäßige Aktualisierung von Systemen und Software

3.3 Zugriffskontrolle

Sicherstellung, dass nur berechtigte Personen auf Daten zugreifen können:

- rollenbasierte Berechtigungskonzepte
- Zugriff nur auf aufgabenbezogen erforderliche Daten
- Protokollierung sicherheitsrelevanter Systemzugriffe
- Einsatz von Firewall- und Netzwerksicherheitsmechanismen

3.4 Weitergabekontrolle

Schutz personenbezogener Daten bei Übertragung oder Weitergabe:

- verschlüsselte Datenübertragung (z. B. TLS / VPN)
- Nutzung sicherer Datenaustauschsysteme
- Protokollierung von Datenübermittlungen
- datenschutzgerechte Vernichtung von Datenträgern

3.5 Eingabekontrolle

Nachvollziehbarkeit der Verarbeitung:

- Protokollierung sicherheitsrelevanter Systemereignisse
- Nachvollziehbarkeit von Datenänderungen
- Systemlogs zur Analyse und Kontrolle

3.6 Auftragskontrolle

Sicherstellung der Verarbeitung gemäß Weisung des Auftraggebers:

- Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung
- vertragliche Regelungen zur Auftragsverarbeitung
- Kontrolle eingesetzter Dienstleister

3.7 Verfügbarkeitskontrolle

Schutz vor Datenverlust oder Systemausfall:

- regelmäßige Datensicherungen
- redundante Systemkomponenten
- unterbrechungsfreie Stromversorgung (USV)
- Einsatz aktueller Virenschutz- und Sicherheitslösungen

3.8 Trennungsgebot

Trennung von Daten unterschiedlicher Auftraggeber und Zwecke:

- logische Trennung innerhalb von Systemen und Datenbanken
- getrennte Berechtigungskonzepte
- auftragsbezogene Datenverarbeitung

4. Überprüfung der Maßnahmen

Die technischen und organisatorischen Maßnahmen werden regelmäßig überprüft und an den Stand der Technik sowie an veränderte Risiken angepasst.