Datenschutz- und Datensicherheitskonzept nach DSGVO

1. Einleitung

Diese Dokumentation beschreibt das Datenschutz- und Datensicherheitskonzept für Docubyte HM GmbH, die vertrauliche Kundendaten im Rahmen der Scan- und Schrifterfassungsdienstleistungen verarbeitet. Ziel ist es, den Schutz personenbezogener Daten gemäß der Datenschutz-Grundverordnung (DSGVO) sicherzustellen.

2. Anwendungsbereich

Dieses Konzept gilt für sämtliche Prozesse und Systeme, die personenbezogene Daten verarbeiten. Dazu gehören insbesondere:

- Datenerhebung,
- Datenverarbeitung,
- Datenspeicherung,
- Datenübermittlung,
- Datenauswertung.

3. Rechtliche Grundlagen

Dieses Konzept basiert auf den Vorgaben der Europäischen Datenschutz-Grundverordnung (DSGVO), insbesondere den Artikeln 5, 6, 13-15, 25, 32, 33 und 35. Zusätzlich werden nationale Regelungen beachtet, insbesondere das Bundesdatenschutzgesetz (BDSG).

4. Verarbeitete Daten

Die Firma verarbeitet folgende Kategorien personenbezogener Daten:

- Kundendaten (Name, Adresse, Kontaktdaten)
- Vertragsdaten (Auftragsinformationen, Leistungsdaten)
- Kommunikationsdaten (E-Mail-Verkehr, Telefonnotizen)
- Erfasste Dokumente und Inhalte (gescannte oder erfasste Schriftstücke)

5. Zwecke der Datenverarbeitung

Die Datenverarbeitung erfolgt zu folgenden Zwecken:

- Vertragserfüllung
- Kundenkommunikation
- Qualitätssicherung
- Archivierung
- Gesetzliche Aufbewahrungspflichten

- Sicherheitsmanagement (Erkennung, Analyse und Verhinderung von Sicherheitsvorfällen)
- Risikomanagement (Einhaltung von Vorgaben zur Datensicherheit und Minimierung von Risiken)
- Statistische Auswertungen und Berichte zur Optimierung der Prozesse
- Forschung und Entwicklung (Analyse anonymisierter Daten zur Verbesserung der Dienstleistung)

6. Technische und organisatorische Maßnahmen (TOMs)

Um die Sicherheit der Daten zu gewährleisten, werden folgende Maßnahmen umgesetzt:

- **Zugriffskontrolle:** Beschränkung der Zugriffsrechte auf autorisierte Mitarbeiter durch ein detailliertes Rollenkonzept
- **Verschlüsselung:** Verschlüsselte Übertragung (z. B. TLS, VPN) und Speicherung sensibler Daten (AES-256)
- **Pseudonymisierung:** Reduktion des Personenbezugs, wo immer möglich
- **Datensicherung:** Regelmäßige, automatisierte Backups auf redundanten, geografisch getrennten Servern
- **Protokollierung:** Aufzeichnung und Überwachung aller Zugriffe auf personenbezogene Daten mit Hilfe von Security Information and Event Management (SIEM)-Systemen
- **Netzwerksicherheit:** Implementierung von Firewalls, Antivirenprogrammen, Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS)
- **Sicherheitsrichtlinien:** Schriftlich dokumentierte Sicherheitsrichtlinien, die regelmäßig aktualisiert werden
- **Sicherheitsaudits:** Regelmäßige interne und externe Audits zur Überprüfung der Maßnahmen
- **Notfallpläne:** Implementierung von Disaster Recovery Plänen für den Katastrophenfall

7. Rechte der betroffenen Personen

Die Firma garantiert betroffenen Personen folgende Rechte:

- Auskunftsrecht (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)
- Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO)
- Recht auf jederzeitigen Widerruf erteilter Einwilligungen (Art. 7 DSGVO)

8. Datenschutzverletzungen

Es werden Maßnahmen implementiert, um Datenschutzverletzungen zu erkennen, zu melden und zu dokumentieren:

- Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnisnahme (Art. 33 DSGVO)
- Benachrichtigung der betroffenen Personen bei hohem Risiko (Art. 34 DSGVO)
- Erstellung eines detaillierten Berichts über Vorfälle und eingeleitete Gegenmaßnahmen
- Regelmäßige Überprüfung und Verbesserung des Sicherheitskonzepts nach Vorfällen

9. Datenschutzfolgenabschätzung

Falls erforderlich, wird gemäß Art. 35 DSGVO eine Datenschutzfolgenabschätzung durchgeführt. Dies erfolgt insbesondere, wenn neue Technologien oder Verfahren eingeführt werden, die erhebliche Auswirkungen auf den Schutz personenbezogener Daten haben könnten.

10. Dokumentation und Überprüfung

Das Datenschutzkonzept wird regelmäßig überprüft und bei Bedarf aktualisiert. Änderungen werden dokumentiert und archiviert. Mindestens einmal jährlich erfolgt eine vollständige Revision. Externe Experten werden regelmäßig zur Validierung der Maßnahmen hinzugezogen.

11. Verantwortlichkeiten

Für die Einhaltung des Datenschutzes ist der Datenschutzbeauftragte der Firma (extern: Firma Verimax GmbH) verantwortlich. Weiterhin sind alle Mitarbeiter verpflichtet, die Datenschutzvorgaben einzuhalten. Schulungen und Sensibilisierungsmaßnahmen werden regelmäßig durchgeführt.

12. Schlusswort

Die Firma verpflichtet sich zur Einhaltung der beschriebenen Maßnahmen und zur kontinuierlichen Verbesserung ihrer Datenschutz- und Datensicherheitsmaßnahmen. Durch regelmäßige Überprüfungen und umfassende Sicherheitsanalysen wird die Wirksamkeit dieses Konzeptes gewährleistet.