KOWOLL PROTECTS
Data Connection & Protection

Checkliste für Datensicherheit gegen den Stand der Technik:

- ☐ Risikobewertung und Schutzbedarfsanalyse: Führen Sie eine gründliche Bewertung der Risiken durch, die mit der Verarbeitung personenbezogener Daten verbunden sind, und legen Sie den Schutzbedarf fest.

- ☐ Informationssicherheitsrichtlinie: Entwickeln Sie eine Richtlinie zur Informationssicherheit, die die Grundsätze, Ziele und Verantwortlichkeiten im Zusammenhang mit Datensicherheit festlegt.

- ☐ Zugangs- und Authentifizierungsmanagement: Implementieren Sie strenge Zugangskontrollen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf sensible Daten haben. Nutzen Sie starke Authentifizierungsmethoden.

- ☐ Verschlüsselung von Daten: Setzen Sie Verschlüsselungstechnologien ein, um Daten während der Speicherung und Übertragung zu schützen.

- ☐ Firewalls und Netzwerksicherheit: Implementieren Sie Firewalls, Intrusion Detection/Prevention Systeme (IDS/IPS) und andere Sicherheitsmaßnahmen, um Netzwerke vor unbefugtem Zugriff zu schützen.

- ☐ Regelmäßige Software-Updates: Stellen Sie sicher, dass Betriebssysteme, Anwendungen und Sicherheitssoftware auf dem neuesten Stand sind, um bekannte Sicherheitslücken zu schließen.

- ☐ Patch-Management: Etablieren Sie einen Prozess zur regelmäßigen Überprüfung, Implementierung und Überwachung von Software-Patches und Updates.

- ☐ Datensicherung und Notfallwiederherstellung: Sichern Sie regelmäßig Daten und entwickeln Sie einen Notfallplan für die Wiederherstellung von Daten nach einem Ausfall oder einer Datenpanne.

- ☐ Physische Sicherheit: Schützen Sie Serverräume und Rechenzentren vor unbefugtem Zugang, Diebstahl oder physischen Schäden.

- ☐ Datensparsamkeit und -minimierung: Reduzieren Sie die Menge der gesammelten und gespeicherten Daten auf das notwendige Minimum, um das Risiko zu minimieren.

- ☐ **Schulung und Sensibilisierung der Mitarbeiter: Sensibilisieren Sie Ihre Mitarbeiter für Datenschutz- und Sicherheitsrichtlinien und schulen Sie sie in bewusstem Umgang mit sensiblen Daten.**

- ☐ Penetrationstests und Sicherheitsaudits: Führen Sie regelmäßig Penetrationstests und Sicherheitsaudits durch, um potenzielle Schwachstellen in Ihrem System zu identifizieren.

- Sicherheitsbeauftragter: Benennen Sie einen Sicherheitsbeauftragten oder ein Sicherheitsteam, das für die Überwachung und Umsetzung der Datensicherheitsmaßnahmen verantwortlich ist.

- Incident Response Plan: Entwickeln Sie einen Plan zur Reaktion auf Sicherheitsvorfälle, um effektiv auf Datenschutzverletzungen oder Sicherheitsverletzungen reagieren zu können.

- Externe Dienstleister und Verträge: Stellen Sie sicher, dass Drittanbieter, die Zugriff auf Ihre Daten haben, ebenfalls angemessene Sicherheitsmaßnahmen implementieren.

Denken Sie daran, dass diese Checkliste als Leitfaden dient und an die spezifischen technologischen und organisatorischen Anforderungen Ihres Unternehmens angepasst werden sollte. Rechtsberatung oder die Unterstützung von IT-Sicherheitsexperten kann dabei hilfreich sein, um sicherzustellen, dass Ihre Datensicherheitsmaßnahmen dem **aktuellen Stand der Technik** entsprechen.