

Datenschutzrichtlinie erstellen

Checkliste für mittelständische Unternehmen

Mit dieser Checkliste erstellen Sie eine professionelle Datenschutzrichtlinie, die alle DSGVO-Anforderungen erfüllt und im Arbeitsalltag funktioniert.

1. Vorbereitung

Anforderungsanalyse durchführen
<input type="checkbox"/> Gesetzliche Vorgaben (DSGVO, BDSG) und branchenspezifische Standards (z.B. TISAX, ISO 27001) für Ihr Unternehmen erfassen.
Internationale Standards prüfen
<input type="checkbox"/> Bei Auslandsgeschäft: CCPA, PIPEDA, HIPAA oder PCI-DSS berücksichtigen und dokumentieren.
Datenschutzziele definieren
<input type="checkbox"/> Mit Geschäftsführung abstimmen: Welche Ziele verfolgen wir? Welche Ressourcen stehen zur Verfügung?

2. Pflichtinhalte dokumentieren

Personenbezogene Daten auflisten
<input type="checkbox"/> Alle Datenkategorien mit konkretem Zweck dokumentieren: Mitarbeiterdaten, Kundendaten, Bewerberdaten.
Verantwortliche benennen
<input type="checkbox"/> Geschäftsführung als Verantwortlicher und Datenschutzbeauftragten mit vollständigen Kontaktdaten angeben.
Betroffenenrechte beschreiben
<input type="checkbox"/> Prozesse für Auskunft, Berichtigung, Löschung, Datenübertragbarkeit und Widerspruch festlegen.
Technische Maßnahmen dokumentieren
<input type="checkbox"/> Verschlüsselung, Firewall, Zugangskontrolle, Backups und weitere Sicherheitsmaßnahmen auflisten.
Organisatorische Maßnahmen festlegen
<input type="checkbox"/> Schulungen, Vertretungsregelungen, Löschkonzepte und Datenschutzprozesse definieren.

<input type="checkbox"/>	Rechtsgrundlagen zuordnen Für jede Verarbeitung die Rechtsgrundlage nach Art. 6 DSGVO festlegen: Einwilligung, Vertrag, Gesetz oder berechtigtes Interesse.
<input type="checkbox"/>	Löschfristen definieren Für jede Datenkategorie konkrete Aufbewahrungsfristen und Löschprozesse festlegen.
<input type="checkbox"/>	Auftragsverarbeiter auflisten Alle Dienstleister dokumentieren und sicherstellen, dass Auftragsverarbeitungsverträge vorliegen.

3. Detailkonzepte ausarbeiten

<input type="checkbox"/>	IT-Sicherheitskonzept erstellen IT-Dokumentation, Verschlüsselung, Passwortrichtlinie, PC-Richtlinie und Firewall-Konzept ausarbeiten.
<input type="checkbox"/>	Datenträgerrichtlinie definieren Umgang mit USB-Sticks, Datensicherung und Cloud-Nutzung regeln.
<input type="checkbox"/>	Mobile-Device-Richtlinie erstellen Regelungen für Smartphones, Tablets und Home-Office mit VPN-Pflicht festlegen.
<input type="checkbox"/>	Zugangs- und Zutrittskontrolle regeln Berechtigungskonzept, Schlüsselmanagement und eventuelle Videoüberwachung dokumentieren.
<input type="checkbox"/>	Notfallplan entwickeln Prozess bei Datenpannen definieren: Meldepflicht binnen 72 Stunden, Verantwortlichkeiten, Sofortmaßnahmen.

4. Umsetzung und Pflege

<input type="checkbox"/>	Geschäftsführung unterzeichnet Finale Datenschutzrichtlinie von Geschäftsführung prüfen und unterzeichnen lassen.
<input type="checkbox"/>	Unternehmensweite Kommunikation Richtlinie per E-Mail, Intranet und Kickoff-Veranstaltung an alle Mitarbeitenden verteilen.
<input type="checkbox"/>	Mitarbeitende schulen

	Präsenzschulungen oder E-Learning durchführen mit Fokus auf praktische Anwendung im Arbeitsalltag.
<input type="checkbox"/>	Jährliche Überprüfung planen Mindestens jährlich auf Aktualität prüfen und bei Änderungen (neue Systeme, Gesetze, Urteile) aktualisieren.

Wichtiger Hinweis:

Diese Checkliste bietet einen Überblick. Für die rechtssichere Umsetzung empfehlen wir die Zusammenarbeit mit einem zertifizierten Datenschutzbeauftragten, der die Richtlinie individuell an Ihr Unternehmen anpasst.

Cortina Consult GmbH | Hafenweg 24, 48155 Münster
Tel: +49 251 95 20 37 - 40 | post@cortina-consult.de | www.cortina-consult.com