Datenschutzpflichten im Überblick

Prüfen Sie systematisch, welche DSGVO-Pflichten für Ihr Unternehmen relevant sind.

1. EU-Vertreter nach Art. 27 DSGVO

☐ Unternehmen ohne EU-Niederlassung, das Waren/Dienstleistungen in der EU anbietet

☐ Unternehmen trackt/analysiert Verhalten von EU-Bürgern (Cookies, Analytics, Tracking)

☐ EU-Vertreter mit Niederlassung in EU benannt und schriftlich beauftragt

☐ Kontaktdaten des EU-Vertreters in Datenschutzerklärung angegeben

2. Datenschutzbeauftragter (DSB)

☐ Mindestens 20 Personen mit automatisierter Datenverarbeitung beschäftigt

☐ Umfangreiche Verarbeitung sensibler Daten (Art. 9/10 DSGVO) als Kerntätigkeit

☐ Datenschutzbeauftragter bestellt und bei Aufsichtsbehörde gemeldet

☐ Kontaktdaten des DSB in Datenschutzerklärung und Impressum veröffentlicht

3. Datenschutzerklärung (Art. 13 DSGVO)

☐ Vollständige Datenschutzerklärung auf Website/in App vorhanden

☐ Verantwortlicher, DSB und ggf. EU-Vertreter mit Kontaktdaten genannt

☐ Zwecke und Rechtsgrundlagen aller Datenverarbeitungen aufgeführt

☐ Betroffenenrechte (Auskunft, Löschung, Widerspruch etc.) vollständig aufgelistet

☐ Speicherdauer oder Kriterien zur Festlegung angegeben

4. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

☐ Verzeichnis aller Verarbeitungstätigkeiten erstellt und aktuell gehalten

☐ Zwecke, Kategorien betroffener Personen und Datenkategorien dokumentiert

☐ Empfänger von Daten (intern/extern) und Drittlandübermittlungen erfasst

☐ Technische und organisatorische Maßnahmen (TOMs) beschrieben

5. Auftragsverarbeitung (Art. 28 DSGVO)

☐ Alle Auftragsverarbeiter identifiziert (Hosting, Cloud, CRM, Marketing-Tools etc.)

☐ Auftragsverarbeitungsverträge (AVV) mit allen Dienstleistern abgeschlossen

☐ Prüfung der Auftragsverarbeiter auf DSGVO-Konformität durchgeführt

6. Technische und organisatorische Maßnahmen (TOMs)

☐ Zugangs-, Zugriffs- und Zugriffskontrollen implementiert

- ☐ Verschlüsselung sensibler Daten (im Ruhezustand und bei Übertragung)
- ☐ Backup- und Wiederherstellungskonzept vorhanden
- ☐ Prozesse für Betroffenenrechte (Auskunft, Löschung etc.) etabliert

7. Datenschutz-Folgenabschätzung (DSFA)

- ☐ Prüfung, ob risikoreiche Verarbeitung vorliegt (Profiling, KI, Tracking, sensible Daten)
- ☐ DSFA bei Bedarf durchgeführt und dokumentiert
- ☐ Datenschutzbeauftragten und ggf. Aufsichtsbehörde konsultiert

8. Weitere wichtige Pflichten

- ☐ Prozess für Meldung von Datenschutzverletzungen (72h-Frist) etabliert
- ☐ Cookie-Banner/Consent-Management bei Einsatz von Tracking-Tools implementiert
- ☐ Mitarbeiter für Datenschutz sensibilisiert und geschult
- ☐ Löschkonzept für personenbezogene Daten vorhanden
