Pflichten der Verantwortlichen Stelle gemäß EU-DSGVO gem. Artikel 24
(Erstellung geeigneter technischer und organisatorischer Maßnahmen)

Folgende Pflichten müssen im Rahmen eines Datenschutzkonzeptes von **jedem Unternehmen und Verein – ganz gleich, wie viele Mitarbeiter / Mitglieder das Unternehmen / der Verein hat**, umgesetzt werden. All diese Forderungen können entweder in Eigenregie oder mit Hilfe eines externen Beraters umgesetzt werden, der die Geschäftsleitung und die Mitarbeiter in der Umsetzung führt und schult.
Wenn mehr als 20 Personen personenbezogene Daten schwerpunktmäßig bearbeiten, **muss** ein **Datenschutzbeauftragter** (intern oder extern) bestellt werden.

- Erstellung und fortlaufende Führung eines Verarbeitungsverzeichnisses inklusive Zuordnung der Rechtsgrundlage, Dokumentation der technischen und organisatorischen Maßnahmen (TOM's) und Information über Löschfristen von Daten

- Erfüllung der Informationspflicht gegenüber Lieferanten, Kunden, Bewerbern und Dritten über Erhebung und Speicherung der verarbeiteten Daten

- Abschluss von Verträgen mit allen Auftragsverarbeitern (AV-Vertrag), Geheimhaltungsvereinbarung mit sonstigen Dienstleistern (z.B. Steuerberater)

- Erstellung von Prozessen
  - Auskunftsrecht
  - Berichtigung von Daten (Revisionsfähigkeit beachten)
  - Einschränkung der Verarbeitung (Zweckgebundenheit)
  - Recht auf Datenübertragung
  - Widerspruchsrecht
  - Mitteilungspflichten
  - Meldung von Datenpannen (Art. 33)
  - Vorgehensweise bei Datenpannen (Incident Response Management)

- Datensicherheitskonzept der eingesetzten Hard- und Software
  (die DSGVO fordert den „Stand der aktuellen Technik" zu nutzen)
  - Übersicht der IT-Infrastruktur (eingesetzte Hardware, Netzwerkplan)
  - Patch-Management
    (wer ist für Updates verantwortlich, wie werden diese sichergestellt und dokumentiert?)
  - Passwort-Management (Vorgaben festlegen)
  - mobile device-Management (Biometrie, E-Mail, Messengerdienste)
  - Backup-Management inkl. Wiedereinspielung von Datensicherungen
    (Recovery-Szenario)
  - Sicherung der USB-Eingänge sowie externer Zugänge
  - Gewährleistung der Datenverfügbarkeit
  - Konzept und Dauer der Datenspeicherung

- Email-Sicherheit, Email-Archivierung, Email-Löschung

- Erstellung von Datenschutzfolgeabschätzungen
  (z.B. bei Verarbeitung sensitiver Daten, neuer Datenverarbeitungsprozesse)

- Zusammenarbeit mit Aufsichtsbehörden

- Erstellung und Umsetzung eines Löschkonzeptes

- Schulung aller Mitarbeiter im Unternehmen in Bezug auf Umgang mit personenbezogenen Daten (pbD) inklusive Sensibilisierung (Awareness) und Aufklärung über mögliche Manipulationsversuche (Social Engineering)

- Verpflichtungserklärungen der Mitarbeiter auf Geheimhaltung und konformen Umgang mit personenbezogenen Daten und externen Datenträgern

- Einverständniserklärungen der Mitarbeiter zur Veröffentlichung von Fotos und Filmaufnahmen

- Beachtung Konformität beim Versand von Newslettern und Werbemaßnahmen

Zur Transparenz gegenüber Dritten trägt zudem die Erstellung eines Leitfadens bei, der beschreibt, zu welchem Zwecke und auf welcher Grundlage die Verarbeitung von Daten erfolgt.

Mit unserem **Know-How** unterstützen wir Unternehmen und Vereine bei der Umsetzung dieser Vorgaben und sehen uns als Coach, der erklärt und anleitet und Sie damit entlastet.

Wenn Sie Fragen zur Vorgehensweise haben oder uns in einem kostenlosen Erstgespräch kennenlernen möchten, freuen wir uns über Ihre Kontaktaufnahme.

corporatr GmbH
Lindpaintnerstraße 88
70195 Stuttgart

+49 (0) 711 13203200
hello@corporatr.com
www.corporatr.com