Datenschutz-Grundverordnung - Checkliste

Mit der am 14.4.2016 vom Europäischen Parlament beschlossenen Datenschutz-Grundverordnung werden die Regeln für die Verarbeitung **personenbezogener Daten**, die **Rechte der Betroffenen** und die **Pflichten der Verantwortlichen** EU-weit **vereinheitlicht**.

Die Bestimmungen der DSGVO gelten ab 25.5.2018. Bis dahin müssen alle Datenanwendungen an die neue Rechtslage angepasst werden. Jedes Unternehmen, das in irgendeiner Weise personenbezogene Daten verarbeitet (z.B. eine Kundendatei führt, Rechnungen ausstellt, Lieferantendaten speichert), ist betroffen. Damit kommen **wesentliche Neuerungen** auf Unternehmen zu.

Die nachstehende Checkliste soll dabei helfen, die erforderlichen Schritte von der Analyse des Ist-Zustandes bis zur Umsetzung eines Maßnahmenplanes rechtzeitig zu setzen:

1. Vorbereitung

- Für die Anpassung an die DSGVO zuständige Personen (intern / extern) nominieren
- Zeit- und Budget-Planung

2. Status – Quo – Erhebung (Analyse des Ist-Zustandes) und Anpassungsbedarf (Soll-Zustand)

- Welche **personenbezogenen Daten** werden verarbeitet?
- Welche **Datenanwendungen** bestehen?
  - Welche **Standardanwendungen** liegen derzeit vor?
  - Welche Datenanwendungen sind derzeit **im DVR registriert**?
  - Überprüfen Sie Ihre AGB, Datenschutzerklärungen, Impressum, laufende Verträge, Website-Einstellungen, etc.
- Was sind die **Zwecke** meiner Datenverarbeitungen?
- Was ist die **Rechtsgrundlage** der Datenverarbeitung?
  - Liegt eine **Einwilligung** vor?
- Welche **sensiblen Daten** werden verarbeitet?
- Werden **Kindern** Dienste der Informationsgesellschaft angeboten?
- Erfolgt **Profiling**?
- Werden **Auftragsverarbeiter** (derzeit „Dienstleister“) herangezogen?
  - Gibt es schriftliche Vereinbarungen für die Auftragsverarbeitung?
  - Weist der Auftragsverarbeiter die erforderliche Zuverlässigkeit auf?
- Wie werden die **Informationspflichten** (nach der DSGVO) erfüllt?
- Wie werden die **Betroffenenrechte** (nach der DSVGO) erfüllt?
  - An wen in meinem Unternehmen können sich betroffene Personen für die Ausübung ihrer Betroffenenrechte wenden?
- Welche **Datensicherheitsmaßnahmen** sind vorhanden?

- Wie ist **privacy by design / privacy by default** implementiert?
- Besteht für meine Datenverarbeitungen **Dokumentationspflicht**?
  - Wie wird die Dokumentationspflicht erfüllt?
- Welche Vorkehrungen gegen **Datenschutzverletzungen** existieren schon in meinem Unternehmen?
- Ist für meine Datenverarbeitungen eine **Datenschutz-Folgeabschätzung** durchzuführen?
  - Welche Risiken aus der Datenverarbeitung ergeben sich für die Rechte und Freiheiten der Betroffenen?
  - Wie kann ich den Risikoeintritt verhindern oder zumindest minimieren?
- Ist eine **vorherige Konsultation** bei der Aufsichtsbehörde notwendig?
- Brauche ich einen **Datenschutzbeauftragten**?
- Welcher **Datenverkehr mit dem EU-Ausland** besteht und auf welcher Rechtsgrundlage?
- Besonderheiten **Arbeitnehmerdatenschutz**
  - Überprüfung von Dienstverträgen, Betriebsvereinbarungen, Dienstordnungen, etc.
  - Rechtzeitige Kommunikation mit dem Betriebsrat
- Wie weise ich nach, dass meine **Datenverarbeitungen DSGVO-konform** erfolgen? (z.B. Dokumentation der Einwilligungserklärungen, Verarbeitungsverzeichnis, Dokumentation der ergriffenen Sicherheitsmaßnahmen, Dokumentation der Risikoabschätzung, Protokollierung oder Dokumentation der Weisungen an dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen, Dokumentation der Verpflichtung der Mitarbeiter des Auftragsverarbeiters zur Vertraulichkeit, etc.).
- Rechtsdurchsetzung und Strafen: **Rechtsbehelfe, Haftungen und Sanktionen**.

3. Maßnahmenplan (für gem. Pkt. 2 identifizierten Anpassungsbedarf)

- Zeitliche und budgetäre Planung (Priorisierung der Ziele)
- Maßnahmen festlegen
- Maßnahmen umsetzen