Die Wichtigkeit einer Datenschutz-Richtlinie bzw. eines Datenschutzmanagementsystems (DSMS)

Warum sind Datenschutz-Richtlinien so wichtig im Unternehmen?

1. Die Europäische Datenschutz-Grundverordnung verlangt in **Artikel 24** der EU-DSGVO von der Unternehmensleitung, sicherzustellen, dass die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt. Dies muss immer nachweislich erfolgen, d. h. mit der sog. **Rechenschaftspflicht.**
2. Um der Nachweispflicht nachzukommen, müssen Verantwortliche **„geeignete technische und organisatorische Maßnahmen“** umsetzen. Diese Maßnahmen müssen sie regelmäßig überprüfen und gegebenenfalls evaluieren.
3. Wie die geeigneten technischen und organisatorischen Maßnahmen genau aussehen, legen **Datenschutz-Richtlinien** fest. In der **Datenschutzerklärung** und in der **Datenschutzrichtlinie** nur auf die Normen der EU-DSGVO zu verweisen, reicht nicht aus. Genauso wenig nützlich ist es, sich lediglich pauschal auf die **Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 DSGVO** zu beziehen.
4. **Datenschutz-Richtlinien** liefern den Beschäftigten im Unternehmen konkrete Vorgaben die es einzuhalten gilt. Sie sind eine Anleitung, wie eine datenschutzgerechte Verarbeitung personenbezogener Daten aussehen sollte.
5. Die Richtlinien sollten dabei den **aktuellen Stand** der Entwicklung der Informationstechnik (IT), der Informationssicherheit und der Risiken für Betroffene berücksichtigen.
6. Die Richtlinien sind u. a. die Basis für **die Unterweisung und Schulung von Beschäftigten** und bilden den Vergleich der Soll- und Ist-Werte einer Datenschutzorganisation ab. Somit ist eine regelmäßige Kontrolle und Evaluierung des Datendatenschutzes erst möglich.
7. Innerhalb eines Unternehmens sind Richtlinien innerbetriebliche Vorschriften (Verfahrens- bzw. Betriebs- oder auch Dienstanweisungen). Die Richtlinien einzuhalten, gehört damit zur Erfüllung des Arbeitsvertrags.
8. Die Richtlinien für den Datenschutz regeln, ***wo von wem und für wen, wobei, wann, wie und warum jemand bestimmte Maßnahmen bei der Verarbeitung personenbezogener Daten ergreifen soll.***

9. Eine Richtlinie für **die Datensicherheit** muss deshalb folgenden Ansprüchen genügen:
    - keine Vorgaben, die Beschäftigte in der Praxis nicht einhalten können.
    - keine ausufernden Konzepte, sondern eindeutige **Hinweise und Regeln.**
    - Richtlinien dürfen sich **nicht widersprechen**.
    - Die Einhaltung **muss nachprüfbar sein**.

10. Was gehört grundsätzlich in ein Datenschutzmanagementsystem:

a. Datenschutzorganisation (Datenschutzkonzept)
b. Datenschutzerklärung(en) (Wichtig Hinweise: Internetseite, Cookies, ggf. Social Media-Nutzung, Betroffenenrechte, ggf. Einwilligungserklärungen für Vertragssituationen, Bildrechte, Beschäftigte etc.)
c. Auftragsverarbeiter-Verträge (AV-Verträge)
   zw. Verantwortlichen und Auftragnehmer
d. Berechtigungskonzept (Zutritt, Zugang, Zugriff)
e. Löschkonzept
   (Akten- und Dokumentvernichtung sowie Löschen von elektronischen Daten)
f. Passwortrichtlinie
g. Schulungskonzept der Mitarbeiter*innen und Koordinatoren für den Datenschutz, Informations- und Datensicherheit)
h. Clean-Desk-Policy (Arbeitsplatzanweisung)
i. Meldung einer Datenpanne (Ablaufplan intern bis zur Aufsichtsbehörde)
j. Verfahrensverzeichnis der Verarbeitungstätigkeiten
   (Verfahrensbeschreibungen)
k. Datenschutz-Folgeabschätzung(en)
l. Informationssicherheitskonzept (z. B. Klassifizierung von Dokumenten, Nutzung von E-Mails, Internet, Hard- und Software, mobilen Datenträgern)
m. Datensicherheitskonzept (z. B. Antiviren-Lösungen, backup-System, Server bzw. Cloud-Lösungen)

Wer kann bei der Erstellung solcher Richtlinien und eines Datenschutzmanagementsystems behilflich sein,

- ✓ ein zertifizierter und professioneller Datenschutzbeauftragter,
- ✓ ein Informationssicherheitsmanager (-beauftragter)
- ✓ ein System-Administrator
- ✓ eine gute IT-Abteilung bzw. ein professionelles IT-Unternehmen