

## „Besteht Beratungsbedarf Datenschutz“

### 1) Geschäftsleitung

- a) Wird das Thema Datenschutz in der Geschäftsleitung „ernst“ genommen?
- b) Gibt es eine Datenschutzrichtlinie im Unternehmen?

### 2) Mitarbeiter

- a) Wurden Mitarbeiter sensibilisiert?
  - Nutzung von Email, Internet und Fax
  - Nutzung unternehmensfremder Hardware
  - Privater Nutzung der Unternehmens-Infrastruktur
  - Erkennen/Bearbeiten von Betroffenenrechten
- b) Kennen die Mitarbeiter die Grundsätze der Verarbeitung personenbezogener Daten nach Rechtmäßigkeit, Treu und Glauben und Transparenz
- c) Liegen Verpflichtungserklärungen zum Datenschutz aller Mitarbeiter vor?
- d) Liegen gesonderte Verpflichtungserklärungen der IT-Administratoren vor?
- e) Erfolgt eine regelmäßige Überprüfung der Einhaltung der Datenschutzvorgaben?

### 3) Technisch-organisatorische Maßnahmen (TOM)

- a) Entsprechen die TOM den aktuellen Vorgaben?
- b) Sind die TOM dokumentiert?
- c) Erfolgt eine regelmäßige Überprüfung der Einhaltung der TOM?

### 4) Auftragsverarbeitung

- a) Sind mit allen Auftragsverarbeitern gültige Vereinbarungen bzgl. der Verarbeitung überlassener personenbezogener Daten abgeschlossen?
- b) Wurden Auftragsverarbeitern auf die DS-GVO-konforme Verarbeitung von personenbezogenen Daten geprüft?
- c) Werden Auftragsbearbeiter in Drittländern eingesetzt und bestehen die entsprechenden Erlaubnistatbestände und Voraussetzungen dafür?

### 5) Verzeichnis der Verarbeitungstätigkeiten

- a) Existiert ein Verzeichnis der Verarbeitungstätigkeiten bezogen auf die Verarbeitung personenbezogener Daten?
- b) Sind Erlaubnistatbestände angegeben (und gültig)?
- c) Sind Löschfristen angegeben?
- d) Sind die Kategorien der verarbeiteten Daten und der betroffenen Personen aufgeführt?

### 6) Außenwirkung

- a) Sind die Datenschutzrichtlinien des Unternehmens klar definiert und in entsprechenden Datenschutzerklärungen gültig formuliert (Webseite, AGB)

### 7) Notfallplan

- a) Existiert ein vorgegebener Notfallplan, der ein klares Verfahren zur Bearbeitung von (ev.) Datenschutzverletzungen für alle Mitarbeiter vorschreibt.
- b) Ist der Notfallplan jedem Mitarbeiter bekannt und kann er von jedem Mitarbeiter eingesehen werden?