

# Implementierung eines Datenschutzmanagements im Unternehmen

## 1. Formale einmalige Aktionspunkte

### 1.1. Bestellung eines betrieblichen oder externen Datenschutzbeauftragten

- Für jede *juristisch selbständige Unternehmenseinheit*.
- Bei mehreren Gesellschaften evtl. als "*Konzerndatenschutzbeauftragter*".

### 1.2. Einbindung in die betriebliche Organisation

- *Unterstellung der Geschäftsführung* bzw. direkte Berichtsmöglichkeit gegenüber der GF.
- *Einbindung in die bestehenden Entscheidungsgremien* im Unternehmen (Lenkungskreise, Management-Circle, Projektsteuerung) und sonstigen Freigabeprozesse (Formulare, Sales- und Marketingaktivitäten).
- U.U. Zusammenarbeit mit dem Betriebsrat oder der Personalvertretung.

### 1.3. Erstellung des öffentlichen Verfahrensverzeichnisses

- Das öffentliche Verfahrensverzeichnis ist "*Jedermann*" auf Antrag zur Verfügung zu stellen.

### 1.4. Realisierung der arbeitsvertraglichen Mitarbeiterverpflichtung

- *Verpflichtung nach § 5 BDSG* (Datengeheimnis) sowie evtl. auf andere Geheimnisse (Betriebs- und Geschäftsgeheimnisse, Fernmeldegeheimnis, Einhaltung EDV-Richtlinien).
- *Belehrung* im formellen Sinne.

## 2. Regelmäßige Aktionspunkte und "nice to have"

### 2.1. Schulungs- oder Sensibilisierungskonzept

- Angebot regelmäßiger *Mitarbeiterschulungen* durch DSB oder Vorgesetzten.
- *Sensibilisierung* durch E-Mails / Artikel im Intranet / Kommerzielle Flyer.
- Regelmäßige *Nachverpflichtung* auf das Datengeheimnis.
- *Kommerzielle Schulungssoftware* (Web-Based-Training) .
- Sonstige *Awarenessmaßnahmen*.

### 2.2. Erstellung der internen Verarbeitungsübersicht

- Manuell z.B. durch *Vorlagen* von BITKOM oder GDD.
- Mittels *spezieller Software* z.B. [DPROREG](#).

### 2.3. Gewährleisten von Datenschutzkonformität

- *Prüfung automatisierter Verarbeitungen* (neue Verarbeitungen im Rahmen der Freigabeprozesse, alte Verarbeitungen im Rahmen von Audits bzw. anlassbezogen).
- Erfüllung der gesetzlich vorgeschriebenen *Vorabkontrollen*.
- Gewährleistung des Datenschutzes bei *Auftragsdatenverarbeitung* (§ 11 BDSG).
- Sicherstellen der *technischen und organisatorischen Maßnahmen nach § 9 BDSG* u.a.

# Implementierung eines Datenschutzmanagements im Unternehmen

## 2.4. Implementieren verbindlichen Unternehmensregelungen und Dokumentation der Datenschutzmaßnahmen

- Entwicklung eines *betrieblichen, individuellen Datenschutzkonzepts*.
- Einführen einer *Sicherheitspolitik* sowie DS- und IT-Security-Richtlinien
- IT-Grundschutz oder andere *Security-Management-Systeme* (ITIL usw.)
- Dokumentation von Prüfmaßnahmen, Freigaben und Stellungnahmen.
- Regelungen zur Protokollierung, vgl. § 31 BDSG.
- Regelungen zur Kontrolle. Abstimmung mit anderen Prozessen (GoBS, KontraG, SOA usw.).

## 2.5. Verfahrensregelungen zum Umgang mit Kunden

- Gewährleisten das Betroffenen ihre Rechte auf *Auskunft, Sperrung, Berichtigung und Löschung* geltend machen können.
- *Privacy Policy* für Internetauftritte entwickeln.
- Regelungen zum Datenschutz in den AGB.
- Datenschutzbrochüren.
- *Zertifizierung* des Datenschutzmanagements.

## 2.6. Fort- und Weiterbildung

- Verbände, Seminare und Erfa-Kreise.