

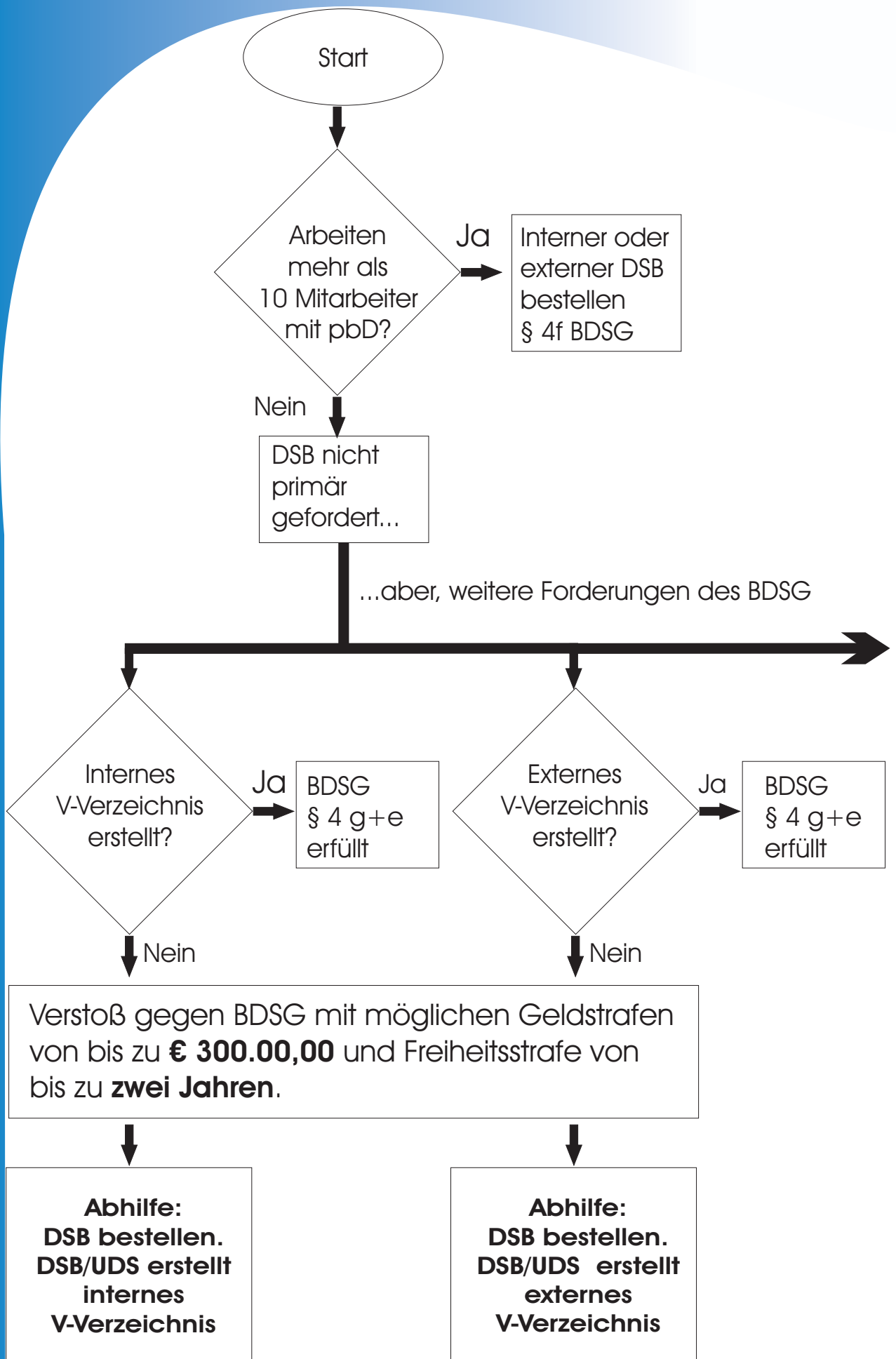
Bundesdatenschutzgesetz (BDSG)

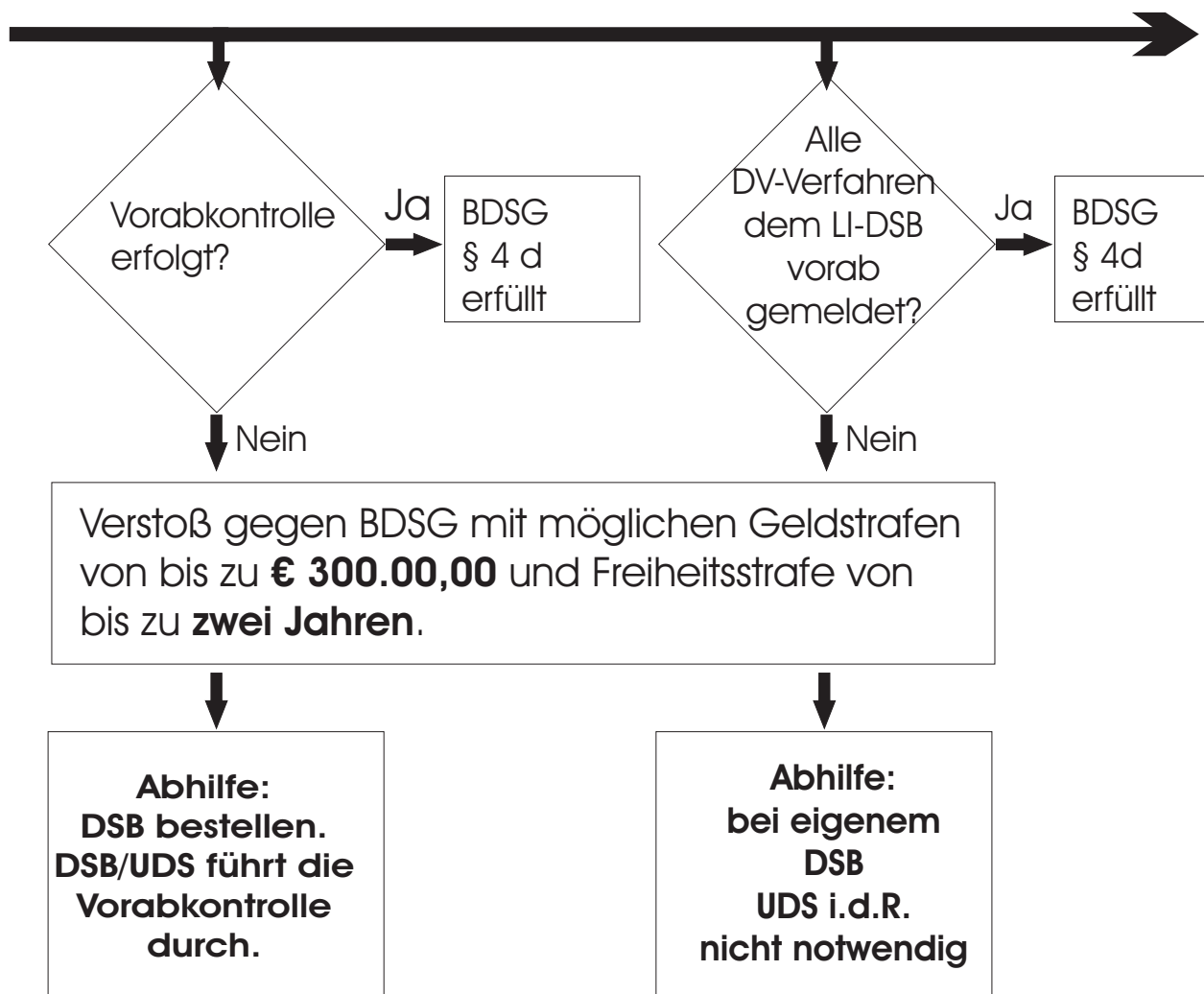
Die wichtigsten Forderungen des BDSG (Auszug)

Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit personenbezogenen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird.

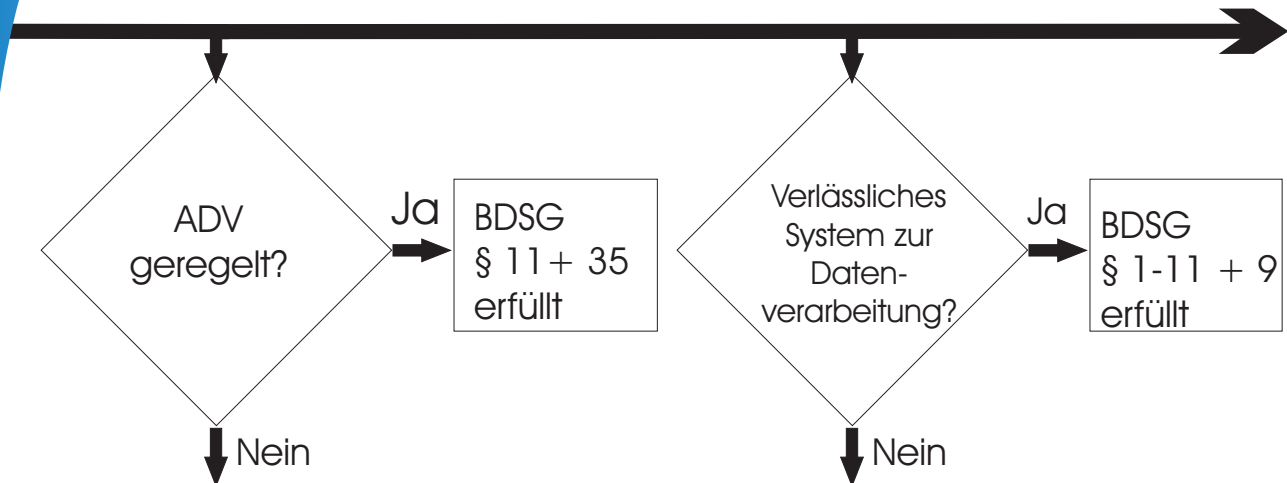
Mitgeltende Gesetze und Verordnungen

- EG Datenschutzrichtlinie 95/46 EG
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Betriebsverfassungsgesetz (BetrVG)





weitere Forderungen des BDSG



Verstoß gegen BDSG mit möglichen Geldstrafen von bis zu **€ 300.00,00** und Freiheitsstrafe von bis zu **zwei Jahren**.

Abhilfe:
DSB bestellen.
DSB/UDS bereitet Verträge mit:

- ◆ EDV Support
- ◆ Lettershop
- ◆ Software-Support
- ◆ Steuerberater

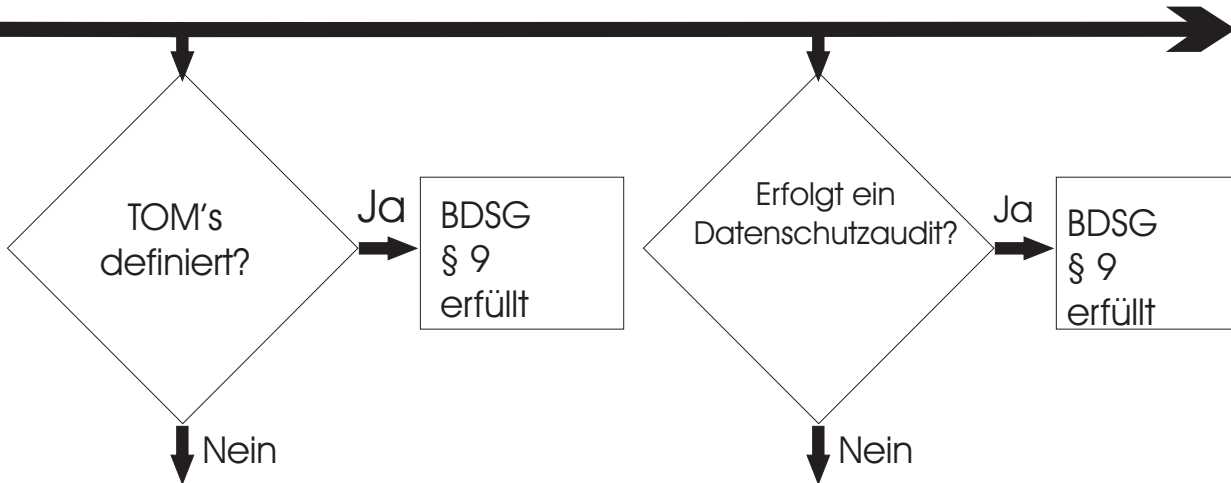
vor.
(Acht Vorgaben sind zu beachten)

Abhilfe:
DSB bestellen.
DSB/UDS stellt sicher, dass die Forderungen hinsichtlich

- ◆ Vertraulichkeit
- ◆ Integrität
- ◆ Verfügbarkeit
- ◆ Authentizität
- ◆ Verbindlichkeit
- ◆ Prüfbarkeit

erfüllt werden.

weitere Forderungen des BDSG



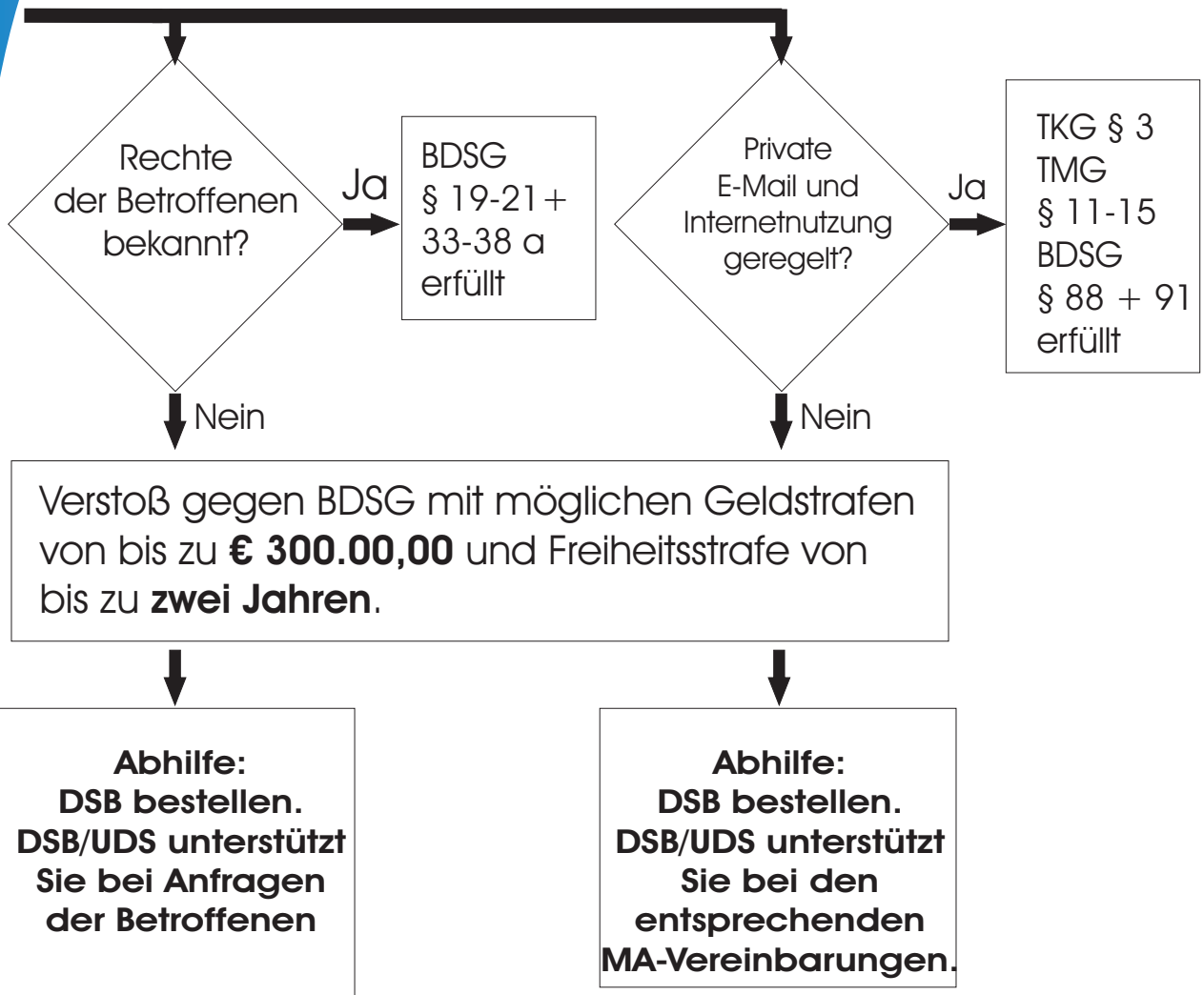
Verstoß gegen BDSG mit möglichen Geldstrafen von bis zu **€ 300.00,00** und Freiheitsstrafe von bis zu **zwei Jahren**.

Abhilfe:
DSB bestellen.
DSB/UDS erstellt mit Ihnen die **technisch/organisatorischen Maßnahmen (TOM's)**
Hinweis:
BSI Handbuch wurde auf unsere Branche angepasst.

- ◆ Zutrittskontrolle
- ◆ Zugangskontrolle
- ◆ Zugriffskontrolle
- ◆ Weitergabekontrolle
- ◆ Eingabekontrolle

Abhilfe:
DSB/UDS bestellen.
Datenschutzaudit lässt sich mit dem internen UDS Audit kombinieren:

weitere Forderungen des BDSG



Informationen zum Datenschutz

Das aktuelle Bundesdatenschutzgesetz (BDSG) begründet sich auf die EG Datenschutzrichtlinie 95/46 EG und der Datenschutznovelle vom 14.08.2009.

Das Bundesdatenschutzgesetz (BDSG) beschreibt im Anwendungsbereich (§1) den Zweck des Gesetzes:

"Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird".

BDSG § 2 "Nicht öffentliche Stellen sind natürliche und juristische Personen; Gesellschaften und andere Personenvereinigungen des privaten Rechts", d.h. auch **Arbeitgeber in der Privatwirtschaft gelten als nicht öffentliche Stellen.** Für die nicht öffentlichen Stellen ist folgender Anwendungsbereich definiert: "Soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten **erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten**" (Auszug BDSG § 1(2)).

BDSG § 4f "**Öffentliche und nicht öffentliche Stellen, die personenbezogenen Daten automatisiert verarbeiten, haben einen DSB schriftlich zu bestellen**". Dies gilt schon seit 1978 so. Bis Herbst 2006 galt diese Regelung, wenn in einem Unternehmen von mehr als vier (also mindestens fünf) Arbeitnehmer personenbezogene Daten erhoben, verarbeitet und genutzt wurden. Um Kleinunternehmen zu entlasten wurde mit dem "Ersten Gesetz zum Abbau bürokratischer Hemmnisse" zwei Änderungen eingeführt:



Die maßgebliche Arbeitnehmerzahl wurde von vier auf **neun** erhöht. Nur Unternehmen in denen mindestens zehn Personen personenbezogene Daten erheben, verarbeiten oder nutzen, müssen einen DSB bestellen

In die Zahl **zehn** werden nur noch Personen eingerechnet, die "**in der Regel**" und "**ständig**" mit personenbezogenen Daten umgehen. Aushilfen und Urlaubsvertretungen und Praktikanten bleiben unberücksichtigt.

BDSG § 3 "Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener).

Personenbezogen Daten können auch Daten von Kunden; Lieferanten; Patienten; Mandanten; Besuchern sein und nicht nur die Daten in oder aus der Personalakte.. Also kann auch der Einkauf; Verkauf, Vertrieb; Sekretariat; Servicetechniker; Montage betroffen sein.

Unabhängig hiervon gelten die Forderungen wie folgt:

Eine **automatisierte Verarbeitung** ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Eine **nicht automatisierte Datei** ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich und ausgewertet werden kann. Anmerkung UDS: Personalakten mit festen Registern und festgelegten Inhalt in den Personal- und Kundenregistern sind deshalb vom BDSG betroffen und werden als automatisierte Verarbeitung angesehen.

Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme der zuständigen Aufsichtsbehörde nach Maßgabe §4 e zu melden.

Die **Meldepflicht entfällt, wenn die verantwortliche Stelle** einen Beauftragten für den Datenschutz **(DSB) benennt** --Auszug BDSG § 4d

Die **Meldepflicht entfällt ferner**, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung; Verarbeitung oder Nutzung personenbezogener Daten beschäftigt ist und entweder eine **Einwilligung des Betroffenen** vorliegt oder die Erhebung; Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen **oder rechtsgeschäftsähnlichen Schuldverhältnis mit dem Betroffenen erforderlich ist.**

Die Meldepflicht entfällt nach Absatz 2 und 3 nicht, wenn es sich um automatisierte Datenverarbeitung zum Zweck der Übermittlung, der anonymisierten Übermittlung oder zum Zweck der Markt - oder Meinungsforschung handelt (neu: BDSG § 30a).

Die Mitarbeiter sind betreffs BDSG regelmäßig zu schulen und auf das Datengeheimnis schriftlich zu verpflichten.

Bei besonderen Daten bei der die Verarbeitung u.a. besondere Risiken für Rechte und Freiheiten der Betroffenen aufweisen, **unterliegt das Verfahren der Vorabkontrolle durch den Beauftragten** für den Datenschutz. **Liegen gesetzliche Verpflichtungen oder die Einwilligung oder des Betroffenen vor** oder die Erhebung; Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines **rechtsgeschäftlichen** oder rechtsgeschäftsähnlichen **Schuldverhältnis** mit dem Betroffenen erforderlich ist, **entfällt die Vorabkontrolle.**

Bei der automatischen Auftragsdatenverarbeitung (ADV) z.B. für externe EDV Dienstleister; externe Sicherheitsdienstleister etc. sind gemäß BDSG § 11 u.a. Gegenstand und die Dauer des **Auftrags; Umfang, Art und Zweck, der Kreis der Betroffenen; Berichtigung, Löschung und Sperrung von Daten vertraglich festzulegen und die Einhaltung der Maßnahmen zu kontrollieren. Die verantwortliche Stelle ist der Auftraggeber.**

Gezieltes Beschaffen von Daten über den Betroffenen gemäß BDSG § 3 umfasst nicht das zufällige Wahrnehmen und die unverlangte Mitteilung Anmerkung (z.B. auf einem -"UDS Seminar")

U.a. fallen auch neben den uns bekannten "Beschäftigten" auch **Bewerberinnen-/ und Bewerber, sowie ausgeschiedene Beschäftigte** in den Begriff von BDSG§ 3

Im Umgang mit den **Internetauftritten / Intranet** und eigenen Onlineshops muss unter Umständen auch das Telekommunikationsgesetz (**TKG**) speziell § 3; § 88; § 91 und das Telemediengesetz, hier **Datenschutzregeln § 11-15 TMG beachtet** werden.

Das Bundesdatenschutzgesetz (BDSG) verlangt und definiert u.a. :
im Anwendungsbereich BDSG § 1

- **Begriffe wie personenbezogene Daten; automatisierte Verarbeitung; Erheben; Verarbeiten; Speichern; Verändern; Übermitteln; Sperren; Löschen; Nutzen; Anonymisieren; Pseudonymisieren etc.**
- **Bestellung** eines internen oder externen Datenschutzbeauftragten (DSB) gemäß BDSG § 4 f und § 4 g (Aufgaben).
- **Ein verlässliches System** das aus technischer Sicht die Forderungen nach: **Vertraulichkeit; Integrität; Verfügbarkeit; Authentizität; Verbindlichkeit und Prüfbarkeit** gewährleistet
- Ein **öffentliches Verfahrensverzeichnis** gemäß BDSG 4 g und 4 e
- Ein **nicht öffentliches Verfahrensverzeichnis** gemäß BDSG 4 g und 4 e
- **Vorabkontrolle** durch die verantwortliche Stelle gemäß BDSG § 4 d **schriftliche Beauftragung zur Auftragsdatenverarbeitung** mit
- Gegenstand und die Dauer des Auftrags; Umfang, Art und Zweck, der Kreis der Betroffenen; Berichtigung, Löschung und Sperrung von Daten gemäß BDSG § 11 und neu: BDSG § 35
- **Technische und organisatorische Maßnahmen** BDSG § 9 (TOM's)
- **Datenschutzaudit** gemäß BDSG § 9 a
- **Allgemeine und gemeinsame Bestimmungen** gemäß BDSG § 1 - 11
- **Regelungen zum Recht des Betroffenen auf Auskunft** BDSG § 34
- **Rechte des Betroffenen** BDSG § 19 - 21 und § 33 - 38 a
- **Allg. Listenprivileg** BDSG § 28 Abs. 3



Was stellt UDS zur Verfügung?

- *Betriebsvereinbarungen zur Internet/E-Mail Nutzung.*
- *Datenschutzunterweisungen aller Mitarbeiter und der Geschäftsleitung.*
- *Vorlagen zur Datenschutzverpflichtungserklärung.*
- *Basispaket technischer und Organisatorischer Maßnahmen*
- *BSI Grundschutzhandbuch angepasst an unseren Kundenkreis*
- *Datenschutzaudit in Verbindung mit unserem internen Audit*
- *Vertragsentwürfe zur ADV*
- *Dienstleistung des externen DSB*
- *Vorlagen zum internen und öffentlichen V-Verzeichnis*