Novellierung des BDSG

Erste Stufe (seit 23.05.2001 in Kraft)

- Umsetzung der EU-Datenschutzrichtlinie
- Angleichung des Datenschutzniveaus in Staat und Wirtschaft
- Neue Instrumente (z. B. Grundsatz der Datenvermeidung und Datensparsamkeit, Vorabkontrolle, Datenschutzaudit)
- Technikregelungen (Chipkarte und Videoüberwachung)

Zweite Stufe

- Umfassende Modernisierung - alles kommt auf den Prüfstand
- Vereinfachung und Verschlankung
- Selbstschutz, Selbstkontrolle, Selbstregulierung
- Transparenz über die Verarbeitung

➔ Vermeidung des Personenbezugs

➔ Verwirklichung der Informationsfreiheit („Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie.“ BVerfGE)

BDSG-Änderungen

- Datenvermeidung und Datensparsamkeit (§ 3a)
- Übermittlung personenbezogener Daten ins Ausland (§§ 4b und 4c) EU = Inland
- Meldepflicht (§ 4d)
- Vorabkontrolle (§ 4e)
- Erweiterte Informationspflichten (§ 4 Abs. 3, § 33 Abs. 1, § 34)
- Regelungen für den Datenschutzbeauftragten (§§ 4f und 4g)
- Bestimmungen zur automatisierten Einzelentscheidung (§ 6a)
- Videoüberwachung öffentlich zugänglicher Räume (§ 6b)
- Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien (Chipkarten) (§ 6c)
- Neue Vorgaben für technische und organisatorische Maßnahmen (§ 9)
- Datenschutzaudit (§ 9a)
- Unterrichtungspflicht bei direkter Werbeansprache über die verantwortliche Stelle und über das Widerspruchsrecht (§ 28 Abs. 4)
- Umgang mit sensitiven Daten (§ 28 Abs. 6 - 9 i. V. m. § 3 Abs. 9)
- Aufsichtsbehörden können generell ohne Anlass kontrollieren (§ 38)

Erhebung nahezu gleich wie öffentl. Bereich

Aufbau des neuen BDSG

Erster Abschnitt (§§ 1 - 11)
- Allgemeine und gemeinsame Bestimmungen -

Zweiter Abschnitt (§§ 12 - 26)
- Datenverarbeitung der öffentlichen Stellen -

Dritter Abschnitt (§§ 27 - 38)
- Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen -

Vierter Abschnitt (§§ 39 - 42)
- Sondervorschriften -

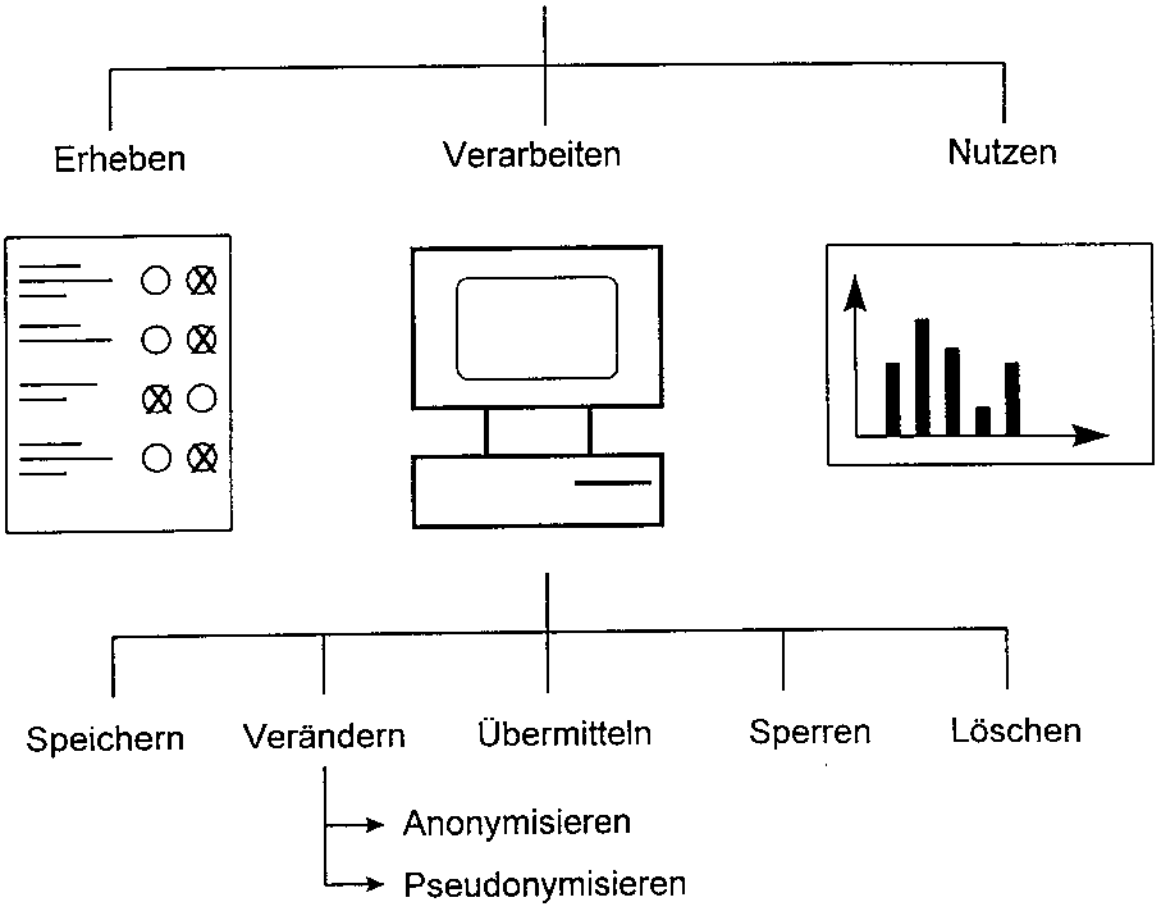
Fünfter Abschnitt (§§ 43 - 44)
- Bußgeld- und Strafvorschriften -

Sechster Abschnitt (§§ 45 - 46)
- Übergangsvorschriften -

keine Strafstunde
Änderung

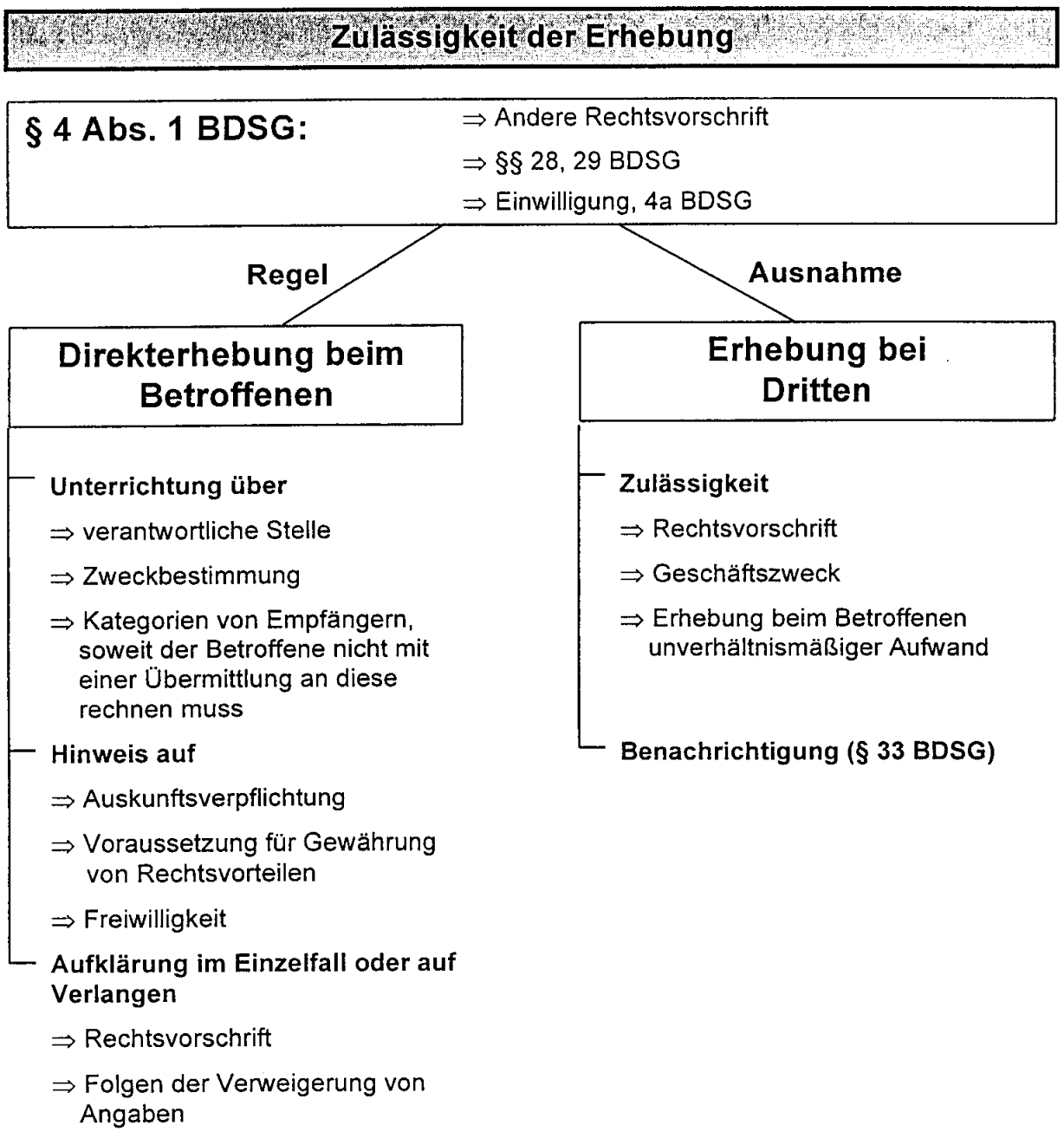
X

Umgang mit personenbezogenen Daten



2. Das Bundesdatenschutzgesetz

Bei der Erhebung personenbezogener Daten sind - unabhängig von der Frage der des allgemeinen Verbots des § 4 Abs. 1 durchbrechenden Zulässigkeitsvoraussetzung - bestimmte in § 4 festgelegte Vorgehensweisen, d.h. der Vorrang der Direkterhebung beim Betroffenen, zu beachten.



Das BDSG schützt grundsätzlich alle personenbezogene Daten, da vom Ansatz her nicht die Art der Daten, sondern ihr Verwendungszweck die Beeinträchtigung der schutzwürdigen Interessen des Betroffenen bewirkt. So ist eine Adresse in der Werbedatei eines Versandhauses weniger problematisch als in der Datei einer Aids-Beratungsstelle; gleichwohl enthält das BDSG für die Verarbeitung bestimmter als besonders „sensibel" bewerteter Daten (§ 3 Abs. 9) und für als besonders gefährdend angesehene Verarbeitungen spezielle Verarbeitungsrestriktionen bzw. Verbote (so für Datenübermittlungen in Staaten außerhalb der EU und des EWR = sog. Drittstaaten (§ 4b u. c) für automatisierte Einzelentscheidungen (§ 6a); für die Videoüberwachung (§ 6b); für automatisierte Abrufverfahren (§ 10)).

2.7 Die Datenübermittlung in Drittländer

Aufgrund der EU-Datenschutzrichlinie haben die EU-Staaten ein weitgehend einheitliches Datenschutzrecht geschaffen. Damit war es gleichzeitig gerechtfertigt, den freien Datenverkehr innerhalb der EU keinen datenschutzrechtlichen Restriktionen zu unterwerfen. Es gilt sogar teilweise das Sitzlandprinzip, d.h. für verantwortliche Stellen, die von Deutschland aus in anderen EU-Ländern Daten erheben, verarbeiten oder nutzen, gilt das BDSG.

Während dem Ziel der EU-Datenschutzrichtlinie entsprechend Datenübermittlungen in Staaten der EU oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (Norwegen, Island, Lichtenstein) so zu behandeln sind, wie derartige Verarbeitungsschritte zwischen inländischen Stellen (§ 4b Abs. 1). Es sind Datenübermittlungen in sog. Drittländer ggf. unzulässig, wenn das Drittland kein angemessenes Datenschutzniveau gewährleistet. Die entsprechende Beurteilung nimmt die übermittelnde Stelle selbst vor, wobei die EU-Kommission insoweit auch allgemeine Feststellungen treffen kann. Kann kein hinreichendes Datenschutzniveau festgestellt werden und liegen auch nicht dem Willen des Betroffenen entsprechende Übermittlungsbefugnisse nach § 4c vor, so kann die übermittelnde Stelle sich den grenzüberschreitenden Datenverkehr einzel- oder fallgruppenbezogen von der obersten Aufsichtsbehörde genehmigen lassen. Voraussetzung für die Genehmigung ist die Schaffung ausreichender Garantien für den Schutz der Betroffenen z.B. durch Vereinbarungen mit dem Datenempfänger.

Die verantwortliche Stelle hat somit bei der Übermittlung in Drittländer - nachdem die Zulässigkeit der Übermittlung nach allgemeinen Datenschutzrecht festgestellt wurde - folgende weitere Prüfschritte vorzunehmen:

Übermittlungen in Drittländer

Besteht ein angemessenes Datenschutzniveau?

1. **Positive Kommissionsentscheidung?**
2. **Positive Entscheidung der verantwortlichen Stelle bezogen auf Drittstaat oder empfangende Stelle nach Kriterien des § 4b Abs. 3 BDSG?**

falls nein

Greifen die Katalogausnahmen des § 4 c Abs. 1 Nr. 1 – 6 BDSG?

falls nein

Genehmigung der Aufsichtsbehörde aufgrund ausreichender Garantien durch Vertragsklauseln oder verbindliche Unternehmensregelungen.

2.8 Die Videoüberwachung

Durch § 6b BDSG wird erstmals auch für nicht-öffentliche Stellen eine eigenständige Rechtsgrundlage zur Videoüberwachung geschaffen. Die Vorschrift ist insofern ein Fremdkörper im BDSG, als dass sie nicht auf die Verarbeitung personenbezogener Daten abstellt, d.h. die erfassten Personen müssen weder bestimmt noch bestimmbar sein. Die Regelung erfasst aber nur die Überwachung sog. öffentlich zugänglicher Räume, d.h. sie gilt also u.a. regelmäßig nicht für Überwachungen am Arbeitsplatz.

Videobeobachtung

Zulässigkeit:

In öffentlich zugänglichen Räumen (= Bereiche) ist die

- **Beobachtung** (längerfristige, nicht einmalige Videofilmaufnahmen; auch bei bloßer Installation, d.h. Möglichkeit der Beobachtung; zur Beseitigung Anspruch aus § 1004 BGB)
- **Verarbeitung und Nutzung (Vorrang hat reine Beobachtung) zulässig im Rahmen der Abwägung der Erforderlichkeit**
  - **zur Wahrnehmung des Hausrechts**
  - **für sonstige konkret festgelegte berechtigte Verwendungszwecke**

Transparenz durch:

- **Erkennbar machen, dass und wer beobachtet**
- **Benachrichtigung des Betroffenen nach § 33, wenn diese Daten Personenbezug erhalten, d.h. einem bestimmten Betroffenen zugeordnet werden**

Löschung der Aufzeichnung:

- **Erforderlichkeit ist entfallen**
- **schutzwürdige Interessen stehen nachträglich entgegen**

<u>Aber:</u> Bei Aufzeichnungen greift das BDSG in vollem Umfang, falls automatisierte Verarbeitung personenbezogener Daten vorliegt.

Meldepflichten

Automatisierte Verarbeitungen sind grundsätzlich vor Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden ... aber

- Die **Meldepflicht entfällt**, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

- Die **Meldepflicht entfällt** ferner, wenn Daten für eigene Zwecke erhoben und dabei höchstens 4 Mitarbeiter beschäftigt sind und Einwilligung vorliegt oder DV der Zweckbestimmung eines Vertragsverhältnisses ... dient.

- **Meldepflicht entfällt nicht** bei automatisierter DV zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung.

Inhalt der Meldung

- Name oder Firma
- Inhaber, Vorstände, Geschäftsführer
- Anschrift der verantwortlichen Stelle
- Zweckbestimmung
- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien
- Empfänger
- Regelfristen für die Löschung
- Datenübermittlung in Drittstaaten
- Beschreibung der Sicherheitsmaßnahmen, um Angemessenheit zu überprüfen

Datenvermeidung

§ 3a Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von DV-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Beispiele:

Prepaid-Karten, Reduzierung des Aufnahmewinkels und Verzicht auf Speicherung bei der Videoüberwachung, anonyme Zahlungsverfahren bei E-Government, anonymes Surfen im Internet

Datenschutzaudit

§ 9a BDSG

Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen können ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.

Kernziele:

- Stärkung der **Selbstverantwortung** und **Stimulierung** des Wettbewerbs
- Verringerung des **Vollzugsdefizits**
- **kontinuierliche Verbesserung** des Datenschutzes und der Datensicherung

§ 6c

Die Stelle, die personenbezogene Speicher- und Verarbeitungsmedien ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten
3. darüber, wie die betroffene Person ihre Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und
4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

Die nach Absatz 1 verpflichteten Stellen haben dafür Sorge zu tragen, dass die zur Wahrnehmung der Rechte nach den §§ 16 und 17 erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

Automatisierte Einzelentscheidung

§ 6a

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

Ausnahmen:

- Abwicklung von Vertragsverhältnissen oder Rechtsgeschäften
- Begehren des Betroffenen wird stattgegeben
- Interessen des Betroffenen sind gewahrt und Betroffener ist informiert

Das **Auskunftsrecht** erstreckt sich auch auf den **logischen Aufbau der automatisierten Verarbeitung**.

Der betriebliche Datenschutzbeauftragte (bDSB)

Neuregelungen

- **Einheitliche Regelungen** für DSB des öffentlichen und nicht-öffentlichen Bereichs (§§ 4f und 4g)
- Pflicht dient einer **qualifizierten Selbstkontrolle**

Neue Aufgaben für bDSB

- Verfahrensbeschreibung auf Antrag „jedermann“ verfügbar machen (§ 4g)
- Vorabkontrolle durchführen, in Zweifelsfällen an die Aufsichtsbehörde wenden (§ 4d Abs. 5 und 6)

Vorabkontrolle

§ 4d Abs. 5 BDSG

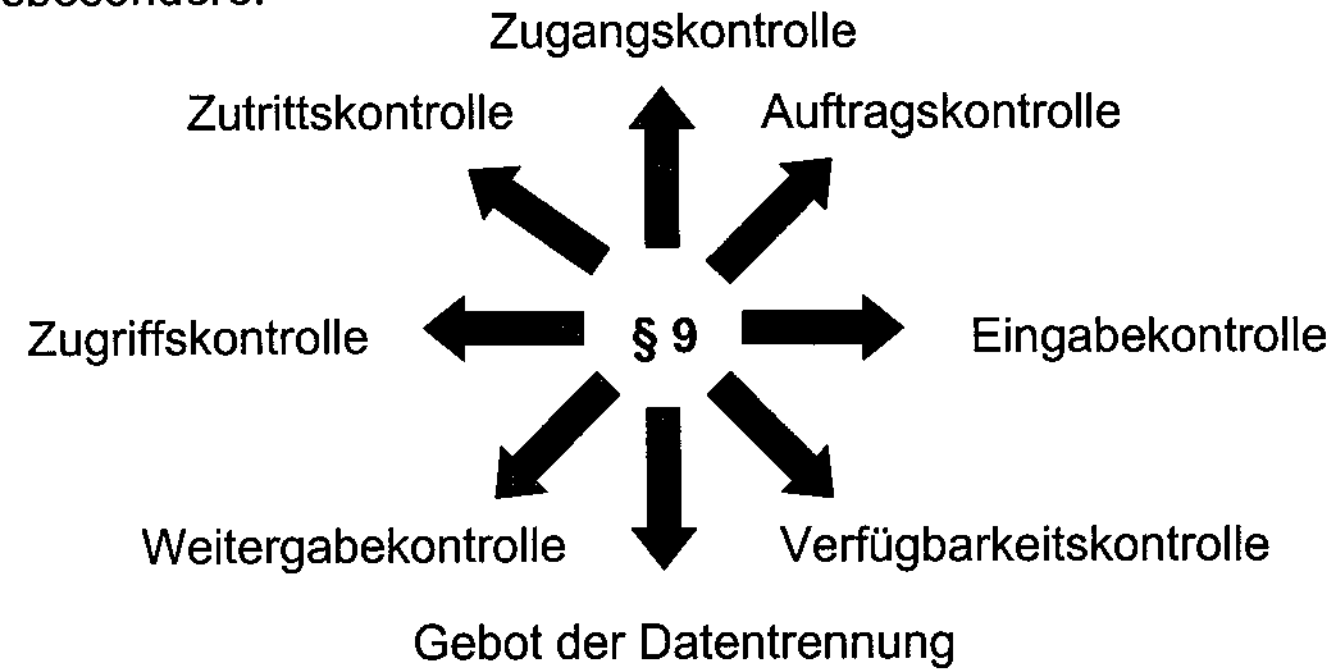
„Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn:

- besondere Arten personenbezogener Daten (sensitive Daten § 3 Abs. 9) verarbeitet werden oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,

es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.“

Datensicherung nach § 9 BDSG und die 8 Gebote

Die innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.
Insbesondere:



Ziele der Datensicherung: ■ Verfügbarkeit ■ Authentizität ■ Integrität

Das Bundesdatenschutzgesetz

Maßnahmen zur Umsetzung der 8 Gebote

- **Zutrittskontrolle**
  - → Zutritt zum Gelände mit Ausweisleser oder Anmeldung beim Pförtner (Besucherschein) oder Operating-Mitarbeiter
  - → Zutritt zum Bandarchiv nur mit Ausweisleser
  - → geschlossenes Gelände mit Kameraüberwachung durch Pförtner
- **Zugangskontrolle**
  - → Zugangsschutzmaßnahmen
  - → Passwortschutz
  - → Verschlüsselung
- **Zugriffskontrolle**
  - → Mehrstufige Firewall-Systeme sichern und prüfen Zugriffe aus dem Intranet und Internet
  - → Protokollierung
  - → Passwortschutz
  - → Berechtigungs- und Betreiberkonzepte
- **Weitergabekontrolle**
  - → Verschlüsselung
  - → Regelung des Kommunikationsverkehrs
  - → Protokollierung

Maßnahmen zur Umsetzung der 8 Gebote

- **Eingabekontrolle**
  - → Sicherungssoftware wie RACF
  - → Protokollierung
  - → Berechtigungskonzept
- **Auftragskontrolle**
  - → Weisungen des Auftraggebers
  - → Betreiberkonzept
  - → Protokollierung
- **Verfügbarkeitskontrolle**
  - → Sicherungskopien an einem anderen Ort
  - → Maßnahmen zum Katastrophenschutz
- **Trennungskontrolle**
  - → logische, keine physische Trennung
  - → Benutzerprofile
  - → Berechtigungen

Aufsichts-Kompetenzen

Die Datenschutzaufsichtsbehörden

- kontrollieren künftig ohne Anlass die Ausführung der Datenschutzbestimmungen, die im Bundesgebiet gelten,
- leisten den Aufsichtsbehörden anderer Mitgliedsstaaten der EU auf Ersuchen Amtshilfe,
- sind befugt, bei der Feststellung von Datenschutzverstößen Strafantrag zu stellen,
- sind befugt, bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zu unterrichten,
- sind befugt, Betroffene über einen Verstoß zu unterrichten,
- führen ein Register der meldepflichtigen automatisierten Verarbeitungen. Das Register kann von jedem eingesehen werden.

Neues BDSG – Was ist nun zu tun?

- Datenvermeidung und Datensparsamkeit
- Meldepflicht
- Vorabkontrolle
- Regelungen für den Datenschutzbeauftragten
- Automatisierte Einzelentscheidung
- Mobile Speichermedien
- Technische und organisatorische Maßnahmen
- Datenschutzaudit
- Kompetenzen der Aufsichtsbehörden