Grundlagen der Datenverarbeitung (VI): Datenschutz und Datensicherheit

Datenschutz

Daten sind **personenbezogen**, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann. Im zweiten Fall spricht man auch von **personenbeziehbaren** Daten.

Beispiele für personenbezogene Daten („Privatsphäre"): Religionszugehörigkeit; Einkommen; Beurteilungen; Familienstand; gesundheitliche Verhältnisse; Kontostand

weitere Datenschutzbestimmungen: ärztliche Schweigepflicht; Steuergeheimnis; Bankgeheimnis; Recht auf Einsichtnahme des Arbeitnehmers in Personalakte

Der Datenschutz umfasst alle Maßnahmen eines Unternehmens, einer Behörde oder sonstigen Organisation zum Schutz aller personenbezogenen Daten vor Missbrauch durch unberechtigte Übertragung und Weitergabe oder unberechtigten Zugriff. Hinzu kommt der Schutz des einzelnen Menschen vor der Sammlung von individuellen Daten über seine Person.

Verpflichtungen und Maßnahmen:

- Schutz personenbezogener Daten durch Unternehmen
  - *Zutrittskontrolle: Unbefugte dürfen keinen Zugang zum Rechenzentrum haben*
  - *Zugangskontrolle: Unbefugte dürfen sich nicht in DV-Anlage einloggen*
  - *Datenträgerkontrolle: Unbefugtes Lesen, Kopieren, Verändern, Entfernen von Datenträgern ist zu verhindern.*
  - *Speicherkontrolle: Unbefugte dürfen weder Daten speichern, verändern oder löschen noch gespeicherte Daten lesen.*
  - *Zugriffskontrolle: Berechtigte dürfen ausschließlich auf Daten zugreifen, die ihrer Zugriffsberechtigung unterliegen.*
  - *Übermittlungskontrolle: Es muss nachweisbar sein, an wen personenbezogene Daten übermittelt werden.*
- Rechte der betroffenen Bürger und Mitarbeiter
  - *Benachrichtigung über Speicherung und Art der gespeicherten Daten*
  - *Auskunft über die gespeicherten Daten, über den Zweck der Speicherung und über die Personen und Stellen, an die seine Daten weitergegeben werden.*
  - *Berichtigung der Daten, wenn die gespeicherten Daten unrichtig sind.*
  - *Sperrung der Daten, wenn weder die Richtigkeit noch die Unrichtigkeit der Daten festgestellt werden kann.*
  - *Löschung der Daten wenn diese unzulässig gespeichert oder nicht mehr benötigt werden.*
  - *Schadenersatz, wenn durch unzulässige oder unrichtige Datenverarbeitung ein Schaden entstanden ist.*
  - *Anrufung des Beauftragten für den Datenschutz bei Bund und Ländern*
- Datengeheimnis
  - *Personen, die mit personenbezogenen Daten zu tun haben, werden zum Schweigen darüber verpflichtet.*
- Technische oder organisatorische Maßnahmen
  - *Diejenigen Betriebe und Einrichtungen, die personenbezogene Daten verarbeiten, haben die geeigneten*
  - *Maßnahmen zu treffen, die den Datenschutz gewährleisten.*

Der betriebliche Datenschutzbeauftragte

Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, sind verpflichtet, bei diesen Arbeiten die Ausführungen des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Die Unternehmen haben einen betrieblichen Beauftragten für den Datenschutz schriftlich zu bestellen, wenn sie bei der automatisierten Datenverarbeitung mindestens 10 Personen oder bei Verarbeitung auf andere Weise mindestens 20 Personen beschäftigen.

Aufgaben des betrieblichen Datenschutzbeauftragten (DSB)

- Auf Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinwirken.
- Die ordnungsgemäßen Anwendungen der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden, überwachen.
- Die bei der Verarbeitung personenbezogener Daten tätigen Personen schulen. Dies kann zum Beispiel in schriftlicher Form, durch Schulungsveranstaltungen oder auch durch Anregungen und Informationen im Rahmen von Dienstbesprechungen erfolgen.
- Jedermann auf Antrag die Angaben über Verfahren automatisierter Verarbeitungen in geeigneter Weise zur Verfügung stellen.
- Vor Beginn der automatisierten Verarbeitung kontrollieren, ob die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist (Vorabkontrolle).

Rechte und Pflichten des DSB

- Die Geschäftsführung hat dem DSB die erforderliche Zeit zur Wahrnehmung seiner Tätigkeit einzuräumen und ihm die Möglichkeit zur eigenen sowie zur Schulung der Mitarbeiter zu geben
- sie hat dem DSB die erforderlichen Mittel wie Hilfspersonal, Geräte u. ä., insbesondere auch eigene Räumlichkeiten zur Verfügung zu stellen
- dem DSB ist eine Übersicht über die Dateien und über die Datenverarbeitungsanlagen bereitzustellen
- bei neuen Projekten im Rahmen der automatisierten Verarbeitung ist der DSB rechtzeitig zu informieren, damit er notwendige Datenschutzaspekte einbringen kann
- der DSB ist der Geschäftsführung disziplinarisch unmittelbar zu unterstellen und es ist ein direktes Vortragsrecht und eine direkte Vortragspflicht sicherzustellen.

Datensicherheit

Die Datensicherung umfasst alle Maßnahmen eines Unternehmens zum Schutz der Daten vor Verlust, Beschädigung, Verfälschung und unerlaubtem Zugriff unberechtigter Personen. Maßnahmen:

- Organisatorische Maßnahmen
  - *Zugangs- und Abgangskontrollen in Computerräumen, z. B. durch offen getragene Ausweise*
  - *bauliche Maßnahmen, z. B. besonders feuergeschützte Räume*
  - *regelmäßige Sicherung der angefallenen Daten auf externe Datenträger*
  - *Großvater-Vater-Sohn- Prinzip (Aufbewahrung von Dateikopien: z. B. heute=Sohn; gestern=Vater; vorgestern=Großvater)*
- Softwaremaßnahmen
  - *Zugangsberechtigung zu Datenendstationen nur über im Programm hinterlegte Passwörter (Zugangscodes)*
  - *Plausibilitätskontrollen bei der Dateneingabe, z. B. bei der Überprüfung der Eingabe anhand vorgegebener Größen (Datum, Preis)*
  - *Prüfziffernverfahren, z. B. bei der EAN-Nummer (letzte Ziffer) bzw. Summen- und Vollständigkeitskontrollen*
- Hardwaremaßnahmen
  - *Zugang zu den Tastaturen und Geräten nur mit Schlüsseln, z. B. an Kassen oder Datenendgeräten*
  - *Überschreibschutz bei Datenträgern*
  - *technische Prüfbitkontrolle bei der Übertragung von Daten*
  - *Notstromaggregat; Parallelrechner; Streamer zur Datenspeicherung, Back-Up-Systeme*

Aufgaben: Lösen Sie die IHK-Aufgaben und weiteren Fragen durch Text- und Internetrecherche

1 Kennzeichnen Sie unten stehende Aussagen mit einer

(1), wenn es sich um Aussagen zur Datensicherung handelt,

(2), wenn es sich um Aussagen zum Datenschutz handelt.

a. Die unberechtigte Übertragung und Weitergabe oder der unberechtigte Zugriff personenbezogener Daten steht hierbei im Vordergrund. ____ ☐

b. Hierbei sollen die Daten selbst vor Verlust, Beschädigung, Verfälschung und unerlaubtem Zugriff geschützt werden. ____ ☐

c. Es handelt sich um Maßnahmen zum Schutz aller personenbezogenen Daten. ____ ☐

d. Die Privatsphäre der Personen soll durch den Missbrauch von Daten geschützt werden. ____ ☐

e. Sämtliche Daten eines Unternehmens sollen durch geeignete Maßnahmen geschützt werden. ____ ☐

f. Dazu gehört auch der Schutz des einzelnen Menschen vor der Sammlung von individuellen Daten über seine Person. ____ ☐

3 Im Rahmen der Datensicherung werden

(1) organisatorische Maßnahmen,
(2) Softwaremaßnahmen,
(3) Hardwaremaßnahmen

unterschieden.

Ordnen Sie den folgenden Maßnahmen zu, um welche Art der Maßnahmen es sich handelt.

a. Zugangsberechtigung zu Datenendstationen nur über Passwörter (Zugangscodes) ____ ☐

b. bauliche Maßnahmen, z. B. besonders feuergeschützte Räume ____ ☐

c. Zugang zu den Tastaturen und Geräten nur mit Schlüsseln ____ ☐

d. Plausibilitätskontrollen bei der Eingabe von Daten ____ ☐

e. Zugangs- und Abgangskontrollen, z. B. durch offen getragene Ausweise ____ ☐

f. regelmäßige Sicherung der angefallenen Daten ____ ☐

g. Summen- und Vollständigkeitskontrollen ____ ☐

h. Prüfziffernverfahren ____ ☐

i. Überschreibschutz bei Magnetbändern oder Floppy-Disks ____ ☐

2 Maßnahmen zu Datensicherung und Datenschutz überschneiden sich zuweilen. Manche Maßnahmen dienen jedoch nur dem Datenschutz, manche nur der Datensicherung.
Kennzeichnen Sie unten stehende Maßnahmen mit einer

(1), wenn diese ausschließlich der Datensicherung dienen,
(2), wenn diese ausschließlich dem Datenschutz dienen,
(3), wenn diese sowohl der Datensicherung als auch dem Datenschutz dienen,
(9), wenn diese weder dem Datenschutz noch der Datensicherung dienen.

a. In einer Programmierabteilung müssen die Mitarbeiter ihre Ausweise mit Zugangsberechtigung offen tragen. ☐

b. Die Mitarbeiter der Personalabteilung haben Zugangsberechtigung zu den Personalstammdaten nur über im Programm hinterlegte Passwörter. ____ ☐

c. Die Datenträger mit den Daten des Tages werden abends in einem feuerfesten Tresor verschlossen. ____ ☐

e. Bei der Übertragung von Daten erfolgt eine technische Prüfbitkontrolle, um „Datensalat" zu verhindern. ____ ☐

f. Neben dem Schreibtischtest führt der Programmierer noch einen Kontrolllauf des Programms mit „harten" Daten durch. ____ ☐

g. Von allen Programmen, die in einem Unternehmen eingesetzt werden, existieren Sicherheitskopien. ____ ☐

h. Das Eingabeprogramm überprüft durch Plausibilitätskontrollen die eingegebenen Daten auf ihre Zutreffendkeit. ____ ☐

i. Ein Bürger verlangt vom Einwohnermeldeamt und der Polizei einen Ausdruck über sämtliche über ihn ggf. gespeicherten Daten. ____ ☐

j. Jede EAN-Nummer ist mit einer Prüfziffer ausgestattet, um nicht zutreffende Erfassungen zu verhindern. ____ ☐

4. Wann ist die Verarbeitung personenbezogener Daten zulässig?
5. Welche Aufgaben hat ein Datenschutzbeauftragter?
6. Welche Verpflichtungen übernehmen Daten verarbeitende Stellen zum Schutz personenbezogener Daten?
7. Welche Rechte hat der Bürger gegenüber den Daten verarbeitenden Stellen?
8. Recherchieren Sie die Themen Gesundheitskarte und digitaler Personalausweis.

1. Wann ist die Verarbeitung personenbezogener Daten zulässig?

Das BDSG formuliert ein Verbot mit Erlaubnisvorbehalt:

DV ist grundsätzlich verboten, es sei denn...
- *der Betroffene gibt sein schriftliches Einverständnis.*
- *es ist per Gesetz ausdrücklich erlaubt.*
  (Verkehrszentralregister, Melderegister, Bundeszentralregister, gesamter Sicherheitsbereich)

2. Welche Verpflichtungen übernehmen Daten verarbeitende Stellen zum Schutz personenbezogener Daten? Nennen Sie drei Verpflichtungen.

⇨ *Zutrittskontrolle*	Unbefugte dürfen keinen Zugang zum Rechenzentrum haben
⇨ *Zugangskontrolle*	Unbefugte dürfen sich nicht in DV-Anlage einloggen
⇨ *Datenträgerkontrolle*	Unbefugtes Lesen, Kopieren, Verändern, Entfernen von Datenträgern ist zu verhindern.
⇨ *Speicherkontrolle*	Unbefugte dürfen weder Daten speichern, verändern oder löschen noch gespeicherte
⇨ *Zugriffskontrolle*	Berechtigte dürfen ausschließlich auf die Daten zugreifen, die ihrer Zugriffsberechtigung
⇨ *Übermittlungsk.*	Es muss nachweisbar sein, an wen pbD übermittelt werden.

3. Welche Aufgaben hat ein betrieblicher Datenschutzbeauftragter? Finden Sie wenigstens vier Aufgaben.

Aufgaben des betrieblichen Datenschutzbeauftragten
- Auf Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinwirken.
- Die ordnungsgemäßen Anwendungen der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden, überwachen.
- Die bei der Verarbeitung personenbezogener Daten tätigen Personen schulen. Dies kann zum Beispiel in schriftlicher Form, durch Schulungsveranstaltungen oder auch durch Anregungen und Informationen im Rahmen von Dienstbesprechungen erfolgen.
- Jedermann auf Antrag die Angaben über Verfahren automatisierter Verarbeitungen in geeigneter Weise zur Verfügung stellen.
- Vor Beginn der automatisierten Verarbeitung kontrollieren, ob die Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist (Vorabkontrolle).

4. Welche Rechte der Bürger gegenüber den Daten verarbeitenden Stellen? Nennen Sie drei Rechte.

⇨ *Benachrichtigung*	über Speicherung und Art der gespeicherten Daten
⇨ *Auskunft*	über die gespeicherten Daten, über den Zweck der Speicherung und über die Personen
⇨ *Berichtigung*	wenn die gespeicherten Daten unrichtig sind.
⇨ *Sperrung*	weder die Richtigkeit noch die Unrichtigkeit der Daten kann festgestellt werden.
⇨ *Löschung*	Daten wurden unzulässig gespeichert oder nicht mehr benötigt werden.
⇨ *Schadenersatz*	wenn durch unzulässige oder unrichtige Datenverarbeitung ein Schaden entstanden ist.
⇨ *Anrufung*	des Beauftragten für den Datenschutz bei Bund und Ländern