

Alles auf Lager

Informationstechnologie

von
Thorsten Lotz

unter Mitarbeit von
Astrid Brose

Winklers 

Alles auf Lager

Das Ihnen vorliegende Buch **Informationstechnologie** aus der Reihe „Alles auf Lager“ beinhaltet alle IT-Themen der ersten beiden Jahre der Ausbildung zur *Fachkraft für Lagerlogistik* und der gesamten zweijährigen Ausbildung zur *Fachlageristin/zum Fachlageristen*. Darüber hinaus ist das Buch nicht nur für den Unterricht in Logistikklassen geeignet, sondern deckt auch wesentliche informationstechnologische Inhalte der Ausbildungen im Groß- und Außenhandel und Einzelhandel sowie der Ausbildung für Büromanagement ab.

Informationstechnologie ist

- **übersichtlich:** Zu Beginn des Buches gibt eine Mindmap den Überblick über die zu erlernenden Inhalte. Um den Schülern die strukturelle Aufbereitung der Inhalte nicht abzunehmen, wurde jedoch auf Zusammenfassungen verzichtet.
- **gut lesbar:** Das Erfassen der Inhalte wird durch eine schülerangepasste Sprache und eine Vielzahl von Bildern und Grafiken unterstützt.
- **praxisnah:** Viele Beispiele mit Praxisbezug ergänzen die theoretischen Inhalte und machen das Buch zu einem wertvollen Ratgeber im Unterricht, bei der Prüfungsvorbereitung und im Berufsalltag.

Zu allen Kapiteln bietet das Buch einen ausführlichen Trainingsbereich mit

- **Einstiegssituationen:** Sie führen zu einem neuen Thema hin, knüpfen an Vorwissen an und erzeugen Motivation und Neugier.
- **Erarbeitungsaufgaben:** Dies sind vertiefende Übungen, die mithilfe der Ausführungen im fachbezogenen Teil gelöst werden können.
- **Trainingsaufgaben:** Die Aufgaben dienen der Wiederholung von wesentlichen Inhalten und befinden sich am Ende eines jeden Kapitels.

Das Buch **Informationstechnologie** wird abgerundet durch eine CD-ROM (BN 5276). Auf dieser CD-ROM befinden sich

- die Lösungen zu allen Aufgaben
- ergänzende Hinweise
- Klassenarbeiten

Für Verbesserungsvorschläge und Anregungen sind Verlag und Autor stets dankbar.

Winklers Verlag, Frühjahr 2014

1. Auflage, 2014
 Druck 1, Herstellungsjahr 2014
 © Bildungshaus Schulbuchverlage
 Westermann Schroedel Diesterweg
 Schöningh Winklers GmbH
 Postfach 33 20, 38023 Braunschweig
service@winklers.de
www.winklers.de
 Lektorat: Kirsten Friedrichs
 Redaktion: Eva Maroske
 Grafik: Claudia Hild, Angelburg
 Layout und Satz: Ottomedien, Hanhofen
 Druck: westermann druck GmbH, Braunschweig
 ISBN 978-3-8045-5275-3

Auf verschiedenen Seiten dieses Buches befinden sich Verweise (Links) auf Internetadressen.

Haftungshinweis: Trotz sorgfältiger inhaltlicher Kontrolle wird die Haftung für die Inhalte der externen Seiten ausgeschlossen. Für den Inhalt dieser externen Seiten sind ausschließlich deren Betreiber verantwortlich. Sollten Sie bei dem angegebenen Inhalt des Anbieters dieser Seite auf kostenpflichtige, illegale oder anstößige Inhalte treffen, so bedauern wir dies ausdrücklich und bitten Sie, uns umgehend per E-Mail davon in Kenntnis zu setzen, damit beim Nachdruck der Verweis gelöscht wird.

Dieses Werk und einzelne Teile daraus sind urheberrechtlich geschützt. Jede Nutzung – außer in den gesetzlich zugelassenen Fällen – ist nur mit vorheriger schriftlicher Einwilligung des Verlags zulässig.

Kapitel 1 Datenschutz und Datensicherheit

1.1	Ziele und Inhalte des Datenschutzes	6
1.2	Persönlichkeitsrecht und Zweckbestimmung	7
1.3	Datenschutz im Unternehmen	7
1.4	Der betriebliche Datenschutzbeauftragte	8
1.5	Datensicherheit bei der Hardware	9
1.6	Datensicherheit bei der Software	9
1.7	Datensicherheit in der Organisation des Unternehmens	10
	Training – Datenschutz und Datensicherheit	11

Kapitel 2 IT-Systeme

2.1	Funktionsweise eines IT-Systems	21
2.2	Speicherung von Daten	22
2.3	IT in der Logistik	24
2.3.1	Logistik-Hardware	24
2.3.2	Netzwerktechnik in der Logistik	25
2.3.3	Software	27
	Training – IT-Systeme	28

Kapitel 3 Tabellenkalkulation mit Microsoft Excel

3.1	Grundlagen von Microsoft Excel	37
3.1.1	Aufbau des Anwendungsfensters	37
3.1.2	Grundlegende Arbeitstechniken	38
3.2	Formeln	40
3.3	Funktionen	41
3.3.1	Funktionsassistent	41
3.3.2	Summenfunktion	42
3.3.3	Auswertungsfunktionen	42
3.3.4	Wenn-Funktion	43
3.3.5	SummeWenn-Funktion	47
3.3.6	Verweis-Funktionen	48
3.4	Datums- und Zeitberechnungen	49
3.5	Diagramme	50
	Training – Tabellenkalkulation mit Microsoft Excel	52

Kapitel 4 Textverarbeitung mit Microsoft Word

4.1	Geschäftsbriefferstellung: DIN 5008	61
4.2	Verwendung von Vorlagen für Dokumente	63
4.3	Serienbriefferstellung	64
	Training – Textverarbeitung mit Microsoft Word	65

Kapitel 5 Präsentationserstellung mit Microsoft PowerPoint

5.1	Visualisierung und Anwendungsgebiete	74
5.2	Entwicklung einer Präsentation	74
5.3	Möglichkeiten der Präsentationserstellung	76
5.4	Grundlegende Bearbeitungstechniken	78
	Training – Präsentationserstellung mit Microsoft PowerPoint	81

BilderBox Bildagentur GmbH, Breitbrunn/Hörsching: 25.2 (Erwin Wodicka);

CASIO Europe GmbH, Norderstedt: 25.1;

DLoG GmbH, Germering: 25.5;

fotolia.com, New York: 24.2 (300dpi), 24.4 (Fatman73), 24 .5 (Peter Atkins), 24 .6 (Scanrail), 81.2 (Brian Jackson);

Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V., München: 25.4;

ICO Innovative Computer GmbH, Diez/Lahn: 25.3;

iStockphoto, Calgary: 24.1 (Spectral-Design);

Jungheinrich AG, Hamburg: 34.1-3;

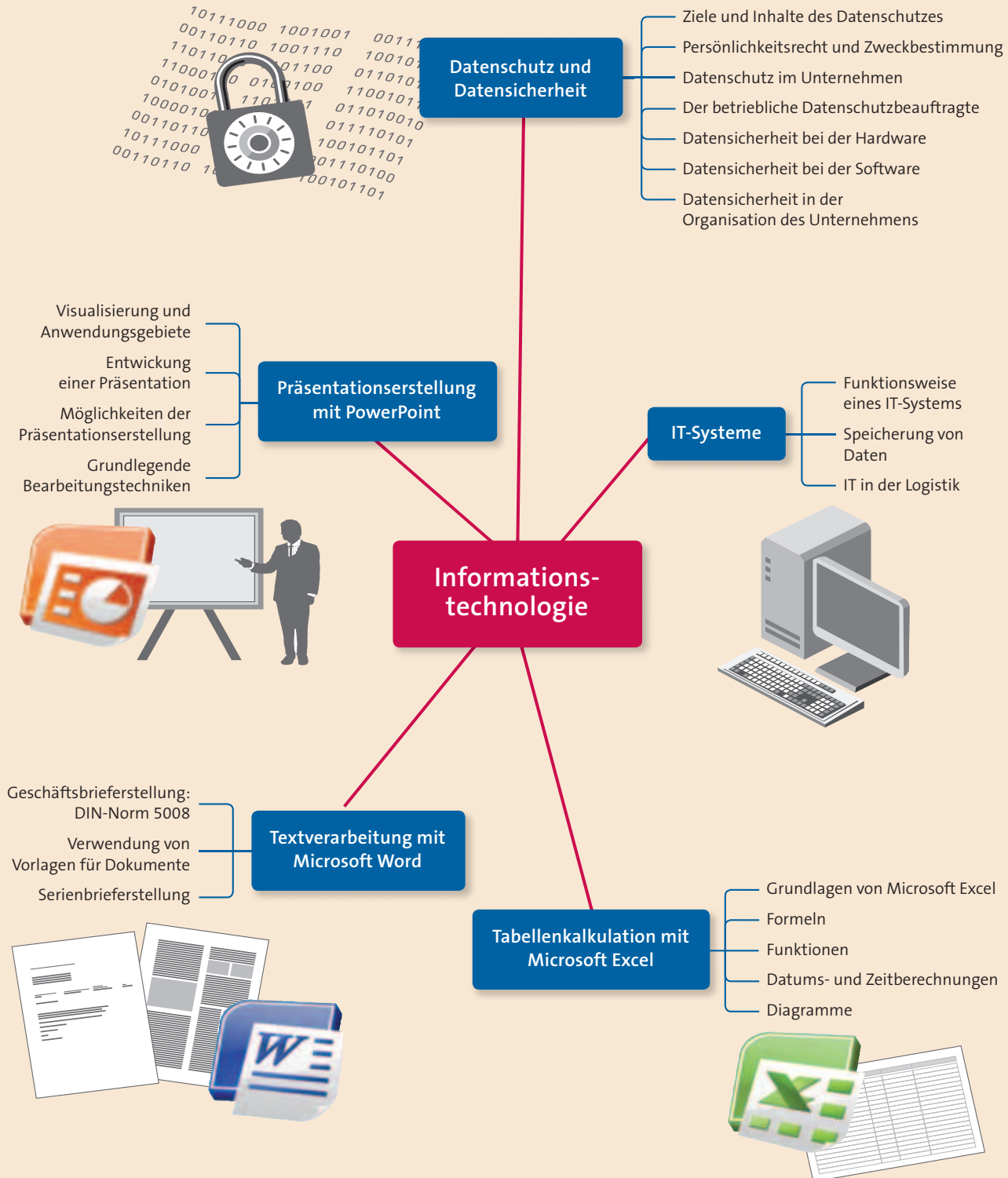
Sony Deutschland, Berlin: 24.3;

toonpool.com, Berlin: 14 (beide) (Jan Tomaschoff und Hannes Richert);

Verlag C. H. Beck oHG, München: 6.1.

alle anderen Illustrationen und Grafiken: Claudia Hild, Angelburg

Informationstechnologie



1 Datenschutz und Datensicherheit

Bundesdatenschutzgesetz (BDSG)

Datenschutz soll die Privatsphäre der Bürgerinnen und Bürger schützen, während Datensicherheit für den Schutz der Hardware, Software und Daten sorgt. Die Datensicherheit ist somit Voraussetzung für den Datenschutz, da ohne effektive Schutzmaßnahmen private Daten leicht an Unbefugte gelangen können.

1.1 Ziele und Inhalte des Datenschutzes

Das Bundesdatenschutzgesetz (BDSG) enthält die Basisregelungen zum Datenschutz in Deutschland. Darin wird in § 1 die Aufgabe des Datenschutzes beschrieben:

§ 1 BDSG

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

Missbrauch persönlicher Daten

Damit steht der Schutz des Menschen vor Missbrauch seiner persönlichen Daten im Zentrum des Bundesdatenschutzgesetzes. Der Missbrauch persönlicher Daten kann auf unterschiedliche Weisen erfolgen, z. B. durch

- fehlerhaftes Erfassen von Daten und Informationen,
- fehlerhaftes Übermitteln von Daten und Informationen,
- unberechtigten Zugriff auf persönliche Daten und Informationen,
- unberechtigte Weitergabe persönlicher Daten und Informationen.

Personenbezogene Daten

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener)“. „Bestimmbar“ kann eine Person dadurch sein, dass man z. B. Einzelangaben aus mehreren Datenbanken so kombiniert, dass erkennbar wird, um welche Person es sich handelt.



Beispiele für personenbezogene Daten

Aufbau des Bundesdatenschutzgesetzes

1. Abschnitt (§§ 1–11)	Allgemeine und gemeinsame Bestimmungen
2. Abschnitt (§§ 12–26)	Datenverarbeitung der öffentlichen Stellen
3. Abschnitt (§§ 27–38 a)	Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen
4. Abschnitt (§§ 39–42 a)	Sondervorschriften
5. Abschnitt (§§ 43–44)	Schlussvorschriften (Straf- und Bußgeldvorschriften)
6. Abschnitt (§§ 45–48)	Übergangsvorschriften



[Information]

[Training]



1.2 Persönlichkeitsrecht und Zweckbestimmung

Nachteile der Daten- und Informationssammlung

Die Datenmenge, die zu jedem Bürger ab seiner Geburt von Ämtern, Unternehmen und Institutionen gesammelt wird, nimmt stetig zu. Ein Überblick ist kaum noch möglich und Probleme mit dem Datenschutz sind vorprogrammiert, wenn zusammenhanglose Daten miteinander kombiniert werden, um Rückschlüsse auf bestimmte Personen zu ziehen.

Vorteile der Daten- und Informationssammlung

Es ergeben sich aber auch vielfältige Vorteile der Daten- und Informationssammlung: Beispielsweise werden Anträge bei Ämtern schneller bearbeitet, beim Arzt ist die Krankengeschichte eines Menschen dokumentiert, der Unternehmer überweist die Löhne und Gehälter an die Mitarbeiter oder jemand bekommt Werbung zugestellt, die auf seine Hobbys abgestimmt ist.

Hieraus werden die gegensätzlichen Interessenlagen deutlich:

- Einerseits hat jeder Mensch das Recht, selbst zu entscheiden, welche persönlichen Daten an andere weitergegeben werden.
- Auf der anderen Seite müssen öffentlich-rechtliche Institutionen (Finanzämter, Bundesagentur für Arbeit, Schulen usw.) und Unternehmen das Recht haben, personenbezogene Daten zu sammeln und zu verwenden, um ihre Aufgaben erledigen zu können.

Zweckbestimmung bei der Datenverwendung

Entscheidend ist immer die „Zweckbestimmung“. Das Bundesdatenschutzgesetz schreibt vor, dass Daten nur dann verarbeitet werden dürfen, wenn dies zur Aufgabenerledigung notwendig ist. So benötigt der Arbeitgeber zur Durchführung der Gehaltsabrechnung bestimmte personenbezogene Daten des Arbeitnehmers, z. B. seine Bankverbindung und seine Anschrift.

1.3 Datenschutz im Unternehmen

Datenerhebung und -speicherung für Geschäftszwecke

Maßgebend ist § 28 BDSG, bei dem es um die „Datenerhebung und -speicherung für eigene Geschäftszwecke“ geht. Im Unternehmen beginnt der Datenschutz

bei Informationen mit einem bestehenden oder herzustellenden Personenbezug, wie es z. B. bei Daten von Kunden und Lieferanten (Anschrift, E-Mail-Adresse, Fotos usw.) der Fall ist. Grundsätzlich gilt bei der Datenerhebung, dass alle Daten, die für einen Vertrag (z. B. Kaufvertrag, Mietvertrag) benötigt werden, erhoben werden dürfen. So darf die Adresse eines Kunden mit Telefon- und Faxnummer beim Warenverkauf erfragt werden. Die Frage nach dem Geburtstag des Kunden oder seinen Hobbys ist dagegen problematisch, denn diese Frage würde vorab eine datenschutzrechtliche Belehrung erfordern.

Arbeitnehmerdaten

Inwieweit Unternehmen Arbeitnehmerdaten verwenden dürfen, richtet sich ebenfalls nach § 28 BDSG. Danach ist es dem Arbeitgeber erlaubt, Arbeitnehmerdaten, die für das Arbeitsverhältnis von Bedeutung sind (Zweckzusammenhang), zu verwenden. Unter anderem gehören Name, Vorname, Geburtsdatum, Beruf, Bankverbindung, Qualifikationen und Einsatzfähigkeit zu den erlaubten Arbeitnehmerdaten. In diese Kategorie fallen auch Arbeitnehmerdaten, die aktuell nicht von Bedeutung sind, es aber in Zukunft sein können. Keinesfalls erhoben und verwendet werden dürfen Informationen über die ethnische Herkunft, private Einstellungen (z. B. zu gesellschaftlichen Themen), sexuelle Orientierungen, politische Meinungen, religiöse Überzeugungen und über die Gesundheit der Arbeitnehmer. Einzig die Frage nach der Religionszugehörigkeit ist wegen der Kirchensteuer zulässig.

Datenschutz und Bewerbungsunterlagen

Zu beachten ist auch, dass Bewerbungsunterlagen eine Reihe personenbezogener Daten enthalten, z. B. Angaben zur Bildung, zum Beruf und zu Zukunftsplänen. Falls ein Unternehmen Bewerber in einem Einstellungsverfahren nicht berücksichtigt, müssen diese Daten, falls sie elektronisch gespeichert wurden, gelöscht werden, denn die Zweckbindung ist nach dem Einstellungsverfahren nicht mehr gegeben. Sollten die Daten auf Papier vorliegen, senden viele Unternehmen die Unterlagen zurück oder vernichten sie.

Die folgende Übersicht stellt dar, unter welchen Bedingungen ein Unternehmen laut BDSG mit personenbezogenen Daten von Betroffenen arbeiten darf. Die automatisierte Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn die Geschäftsführung folgende Maßnahmen gewährleisten kann:

[Information]

[Training]

Erforderliche Maßnahmen	Beispiele für die Umsetzung
1. Zutrittskontrolle	Gebäude- und Raumzugänge zu IT-Systemen regeln
2. Zugangskontrolle	Passwörter und PC-Sperrungen verwenden
3. Zugriffskontrolle	Zuständigkeiten zur Benutzung eines IT-Systems festlegen; mit Lese-, Schreib- und Löschberechtigungen arbeiten
4. Weitergabekontrolle	E-Mails und Netzwerkverkehr verschlüsseln
5. Eingabekontrolle	Veränderungen an Dateien protokollieren, Zugriffs- und Tätigkeitsprotokolle („Logfiles“) vom System erstellen lassen
6. Auftragskontrolle	Vorgaben des Auftraggebers einhalten
7. Verfügbarkeitskontrolle	regelmäßige Datensicherungen („Back-ups“) durchführen, Notfallhandbücher erstellen
8. Trennungskontrolle	Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeiten (Protokolle anfertigen, Kontrollen durchführen)

1.4 Der betriebliche Datenschutzbeauftragte

Bundes-, Landes- und Institutionenebene des Datenschutzes

Datenschutzbeauftragte gibt es sowohl auf Bundesebene (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, www.bfdi.bund.de) als auch auf Landesebene. Auf der Institutionenebene (Betriebe, Behörden, Unternehmen) werden ebenfalls Zuständige für den Datenschutz benannt.

Aufgaben und Stellung des betrieblichen Datenschutzbeauftragten (bDSB)

So haben nach § 4 f Abs. 1 BDSG „öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für Datenschutz schriftlich zu bestellen“. Der betriebliche Datenschutzbeauftragte (kurz „bDSB“) hat primär die Aufgabe, Transparenz in der unternehmensbezogenen Datenverarbeitung zu schaffen und die Einhaltung des BDSG und anderer Datenschutzvorschriften zu kontrollieren. Hierzu gehört auch die Überwachung von Hardware und Software, mit deren Einsatz personenbezogene Daten verarbeitet werden. Außerdem kommt dem bDSB die Aufgabe zu, die bei der Verarbeitung personenbezogener Daten tätigen Personen über datenschutzrechtliche Vorschriften zu informieren. Ferner ist der bDSB auch Anlaufstelle für Mitarbeiter, die Verletzungen ihrer persönlichen Datenschutzrechte befürchten. Natürlich ist der bDSB zur Verschwiegenheit verpflichtet, auch gegenüber dem Unternehmer. Nicht zuletzt muss er bei allen datenschutzrechtlichen bedeutsamen Aktivitäten hinzugezogen werden.

Der bDSB ist der Unternehmensleitung zwar direkt unterstellt, aber in Bezug auf Datenschutzaspekte nicht an Weisungen gebunden. Falls es Klärungs- und Gesprächsbedarf gibt, vermittelt er zwischen dem Unternehmen und der übergeordneten Aufsichtsbehörde, z. B. dem Landesbeauftragten für Datenschutz. Falls sich im Unternehmen kein geeigneter Kandidat für das Amt findet, kann auch eine externe Person mit der nötigen Fachkenntnis zum bDSB bestellt werden. Eine wesentliche Pflicht des Unternehmers gegenüber dem bDSB besteht darin, ein „Verfahrensverzeichnis“ des Unternehmens bereitzustellen, das über Ziele, Struktur und Ablauf der Datenverwendung informiert.

Bestellung des betrieblichen Datenschutzbeauftragten

Jedes Unternehmen muss einen bDSB bestellen, wenn der Betrieb „automatisiert“, also mithilfe von IT-Technik, personenbezogene Daten erhebt und verarbeitet. Eine Ausnahme gilt, wenn nicht mehr als neun Arbeitnehmer beschäftigt werden, die IT-Aufgaben ausführen. Diese Mitarbeiter müssen aber solche Aufgaben nicht ständig erledigen. Ein Beispiel dafür ist die Sekretärin, die unter anderem auch mit Kundendaten arbeitet. Eine weitere Ausnahme gibt es, wenn ein Betrieb Daten ausschließlich auf andere Weise verwendet, etwa auf Papier, Karteikarten usw. Dann müssen mindestens 20 Personen mit der Verwendung personenbezogener Daten beschäftigt sein. Dabei zählen auch Teilzeitkräfte und Auszubildende zu diesem Personenkreis.



Ein bDSB muss unabhängig von der Beschäftigtenzahl immer benannt werden, wenn besondere personenbezogene Daten automatisiert verarbeitet werden, wie z. B. Informationen über politische Meinungen, religiöse Überzeugungen oder die Gesundheit der Mitarbeiter. Wenn die oben genannten Voraussetzungen vorliegen, ist der bDSB spätestens innerhalb eines Monats nach Aufnahme der Geschäftstätigkeit des Unternehmens zu berufen.

Datensicherheit

Datensicherheit umfasst alle Maßnahmen zur Verhinderung von Datenmanipulationen, Datenverlusten, unberechtigten Datenzugriffen sowie Datenmissbrauch. Übergeordnet kann man auch von „Sicherheit in der Informationstechnik (kurz: „IT-Sicherheit“)“ sprechen. Um Datensicherheit im Unternehmen vollständig zu gewährleisten, müssen die entsprechenden Maßnahmen die Bereiche Hardware, Software und Organisation abdecken.

1.5 Datensicherheit bei der Hardware

Maßnahmen für die Datensicherheit bei der Hardware umfassen die Technik, also die eigentliche Computerhardware, die Wartung der im Unternehmen genutzten Computer sowie spezielle Vorkehrungen.

Technik

Technische Maßnahmen beziehen sich zum einen auf die Computerhardware im engeren Sinne. Hier sollte man im Unternehmen immer hochwertige Technik einsetzen. Auf der anderen Seite fallen auch Einrichtungen in diese Rubrik wie z. B. Datensicherungscomputer (Back-up-PCs), die parallel betrieben werden, und Notstromversorgungen, um bei einem Stromausfall ein reguläres Herunterfahren der Anlage zu ermöglichen.

Wartungen

Unerlässlich sind regelmäßige Wartungen der Anlagen und der Netzwerktechnik sowie die frühzeitige Erkennung, Bewertung und Beseitigung von Störungen.

Spezielle Vorkehrungen

Brandschutzvorrichtungen, Diebstahlsicherungen und Hochwasserschutz können die technischen Maßnahmen sinnvoll abrunden.

1.6 Datensicherheit bei der Software

Maßnahmen für die Datensicherheit bei der Software umfassen die Verwendung von Passwörtern und passwortgeschützten Bildschirmschonern, von Virenschern, einer Firewall und Sicherheitseinstellungen sowie das Protokollieren von Fehlern, die Verschlüsselung von E-Mails und Dokumenten und die regelmäßige Aktualisierung der Software.

Passwörter

Die Datensicherheit bei der Software kann beispielsweise dadurch verbessert werden, dass die Anwender für die Anmeldung an das System sichere Passwörter eingeben müssen und diese Zugriffe gespeichert werden. Diese Daten stehen dann für Kontrollen zur Verfügung. Hier kann auch vom Systemverwalter vorgeschrieben werden, dass Passwörter in bestimmten Abständen zu ändern sind.

PC-Sperre

Eine relativ einfach umzusetzende Sicherheitsfunktion ist das Sperren des PC bei Abwesenheit, insbesondere in Verbindung mit einem passwortgeschützten Bildschirmschoner, der nach kurzer Zeit automatisch aktiviert wird.

Fehlerprotokolle

Mithilfe von Software lassen sich die in einem IT-System auftretenden Fehler protokollieren und analysieren.

Virenschanner

Ein wichtiger Softwareschutz zur Erhöhung der Datensicherheit stellt die Verwendung eines aktuellen Virenschanners dar, also eines Programms, das „Schadlingsprogramme“, die zu Datenverlusten führen können, ausfindig macht und löscht. Bekannte Unternehmen, die Virenschutzsoftware vertreiben, sind z. B. G Data, Kaspersky, Norton, Avira und Norman.

Firewall

Eine Firewall („Brandmauer“) hat die Aufgabe, ein zu schützendes Netzwerk vom Internet abzuschirmen. Das geschieht durch Beschränkung des Datenverkehrs, wobei nur Daten durchgelassen werden, die bestimmte Sicherheitsregeln erfüllen. Bei vielen Virenschutzprogrammen gehört eine Firewall zum Lieferumfang.

Verschlüsselung

Eine weitere Möglichkeit besteht darin, E-Mails und Dokumente per Software zu verschlüsseln (chiffrie-

[Information]

[Training]

ren), damit die darin enthaltenen Informationen nur von den berechtigten Personen gelesen werden können. Ein weitverbreitetes Programm dieser Kategorie ist PGP („Pretty Good Privacy“: „Ziemlich Gute Privatsphäre“).

Softwareaktualisierung

Wichtig ist es außerdem, Software immer auf dem aktuellen Stand zu halten und regelmäßig Aktualisierungen („Updates“) durchzuführen. Dadurch werden auch bestehende Sicherheitslücken geschlossen.

Sicherheitseinstellungen

Nicht zuletzt können in allen Webbrowsern (z.B. Internet Explorer, Firefox, Opera, Safari, Chrome) „Sicherheitsstufen“ (von niedrig bis hoch) für bestimmte Internetzonen gewählt werden (Menüfolge beim Internet Explorer: Extras → Internetoptionen → Register „Sicherheit“).



Sicherheitsstufen beim Internet Explorer

1.7 Datensicherheit in der Organisation des Unternehmens

Organisatorische Maßnahmen für die Datensicherheit im Unternehmen umfassen Zutrittskontrollen, das Standardisieren betrieblicher Abläufe, die Ablaufplanung für Datensicherungen und ein gut ausgearbeitetes Datensicherheitskonzept.

Zutrittskontrollen

Wirksam sind Zutrittskontrollen der Mitarbeiter für bestimmte Unternehmensbereiche mithilfe elektronischer Ausweise.

Standardisierungen

In die Kategorie der organisatorischen Maßnahmen fällt das Standardisieren und Protokollieren von betrieblichen Abläufen. Standards, die allen Mitarbeitern bekannt sind, stellen in diesem Zusammenhang immer eine Sicherheitsverbesserung dar.

Datensicherungen

Organisatorisch unabdingbar ist eine klar geregelte Ablaufplanung für die Durchführung von Datensicherungen (Back-ups), also für das Kopieren von Daten auf einen anderen Computer oder ein anderes Speichermedium (z.B. USB-Stick, externe Festplatte, DVD). Dabei muss von vornherein feststehen, wann von wem welche Daten wohin gesichert werden. In der Praxis ist es natürlich sinnvoll, diese Prozesse zu automatisieren und die Datensicherungen – je nach Wichtigkeit der Daten – in bestimmten Zeitintervallen durchzuführen. Die Datenträger selbst sollten immer räumlich getrennt aufbewahrt werden.

Datensicherheitskonzept

Grundsätzlich sollte in jedem Unternehmen ein Datensicherheitskonzept vorliegen, das konkrete Risiken und Bedrohungen benennt und – davon abgeleitet – alle getroffenen Maßnahmen und personellen Zuständigkeiten beschreibt. Es ist sinnvoll, dass ein solches Konzept auch Checklisten beinhaltet, die für Überprüfungen herangezogen werden können.



Training – Datenschutz und Datensicherheit, Kap. 1.1 bis 1.4

Einstiegssituation: Ein Tag wie jeder andere?!

Anja Schön macht eine Ausbildung zur Fachkraft für Lagerlogistik. Vor Beginn ihrer Arbeit geht sie noch in den Supermarkt, holt sich etwas zu essen und bezahlt mit ihrer Bankkarte. Nach zwei Stunden Arbeit soll sie in die Personalabteilung kommen, um ihr Zeugnis für eine absolvierte Weiterbildung abzuholen. Außerdem kann sie dort gleich ihre neue Bankverbindung bekanntgeben.

Aufgrund eines Arzttermins beendet sie heute ihre Arbeit im Betrieb früher als gewöhnlich. Bevor sie das Werksgelände verlässt, stempelt sie natürlich aus. Da sich der Bus deutlich verspätet, steht fest, dass sie den Termin nicht einhalten kann. Zum Glück hat sie ihr Handy dabei, sodass sie die Arztpraxis kontaktieren und eine Terminverschiebung um 30 Minuten vereinbaren kann.

Der Bus erscheint endlich: Anja Schön zeigt dem Fahrer ihre Monatskarte und nimmt einen Platz ein. Die letzten Meter zur Praxis legt sie zu Fuß zurück. Plötzlich sieht sie, wie ein Polizist einen jungen Mann aus einem Kaufhaus führt und ihn zum Streifenwagen bringt. Am nächsten Tag liest sie hierüber in der Zeitung, dass es sich um einen Ladendieb handelte, der durch die Aufnahmen einer Überwachungskamera des Marktes überführt werden konnte.

In der Arztpraxis angekommen, legt sie ihre Krankenversicherungskarte vor und die Behandlung am rechten Fußgelenk kann beginnen. Nach dem Arzttermin macht sie sich auf den Nachhauseweg und

sieht dabei unter anderem, dass Verkehrspolizisten Parksünder aufschreiben und in der Fußgängerzone eine Umfrage gemacht wird.

Zu Hause setzt sie sich gleich an die Hausaufgaben, denn am nächsten Tag ist Berufsschule. Für ein Referat sucht sie noch nach fehlenden Informationen im Internet. Beim Surfen wird ihr die Teilnahme an einem Preisausschreiben angeboten und sie macht mit. Um 18:00 Uhr kommt ihr Vater nach Hause und berichtet vom neuen Arbeitsvertrag, den er heute abgeschlossen hat. Er ist schon ganz aufgeregt, weil morgen sein erster Arbeitstag in dem neuen Unternehmen ist.

Nach dem Abendessen setzt sich Anja noch einmal an den PC, liest ihre E-Mails, schaut nach neuen Kontakten bei azubibook.com und meldet sich schließlich noch bei buy-e an, weil sie CDs verkaufen möchte. Da sie morgen früh aufstehen muss, geht sie danach zeitig ins Bett.

1. An welchen Stellen wurden von Anja Schön oder anderen Personen an diesem Tag persönliche Daten hinterlassen?
2. Vergleichen Sie diese Auflistung mit den Daten, die Sie persönlich an einem „ganz normalen Tag“ hinterlassen. Wo gibt es Überschneidungen, wo Unterschiede?
3. Welche Daten sollten Ihrer Ansicht nach besonders geschützt werden? Begründen Sie Ihre Antwort.

Erarbeitungsaufgaben

1. Formulieren Sie zu den folgenden Behauptungen jeweils ein Pro- und ein Kontra-Argument:

a) „Der Datenschutz hilft, in unserer vernetzten Welt den gläsernen Menschen wirksam zu verhindern.“

.....

.....

.....

.....

.....

[Information]

[Training]

b) „Vor dem Missbrauch meiner Daten habe ich keine Angst – Datenschutz ist überflüssig.“

.....

.....

.....

.....

.....

c) „Datenschutz ist gut gemeint, aber ich traue keinem Gesetz, sondern passe lieber selber auf.“

.....

.....

.....

2. Themen des Datenschutzes werden in der Gesellschaft kontrovers diskutiert, z. B.:



Mitarbeiterüberwachung



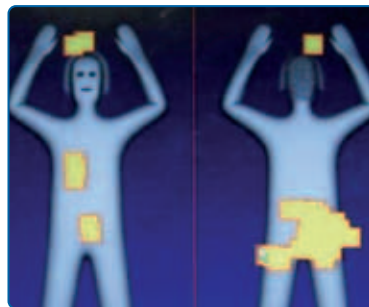
Google Street View



Biometrischer Personalausweis



Kundendaten



Körperscanner



NSA-Affäre

a) Führen Sie zu den Themen eine Internet-Recherche durch und beschreiben Sie die jeweilige Problematik.

.....

.....

.....

.....

.....



b) In welcher Weise ist der Datenschutz betroffen?

.....

.....

c) Beschreiben Sie Ihre eigene Sichtweise zu den oben genannten Fällen.

.....

.....

.....

d) Welche aktuellen Beispiele fallen Ihnen zum Datenschutz noch ein? Stellen Sie Ihre Ergebnisse im Rahmen eines Vortrages mit Präsentation Ihrer Klasse vor.

(Hinweis: Die Seite www.projekt-datenschutz.de liefert eine Vielzahl von Beispielen und Anregungen.)

.....

.....

.....

3. Ergänzen Sie den Lückentext zum Datenschutz, indem Sie die folgenden Begriffe einfügen:

- | | |
|-------------------------------|----------------------------------|
| • Basisregelungen | • Löschung/Entfernung |
| • Bundesdatenschutzgesetz | • Missbrauch |
| • Bundesländern | • Personen (Betroffene) |
| • Daten | • Recht |
| • Erhebung/Erfassung/Sammlung | • Verwendung/Nutzung/Speicherung |
| • Gesetze | |

Das BDSG (.....) enthält die zum
Datenschutz in Deutschland. Darauf aufbauend gibt es in den jeweils
eigene Das BDSG selbst schützt keine, son-
dern davor, dass mit ihren Daten be-
trieben wird. Jeder Bürger hat das, selbst über die
..... ,
oder seiner Daten zu entscheiden.

4. a) Nennen Sie konkrete Beispiele, in denen Sie in Ihrem Ausbildungsbetrieb mit dem Datenschutz in Berüh-
rung kommen oder gekommen sind.

.....

.....

.....

b) Hat Ihr Ausbildungsbetrieb einen betrieblichen Datenschutzbeauftragten?

.....

[Information]

[Training]

5. Erklären Sie die gegensätzlichen Interessen von Privatpersonen und Unternehmen bei der Datenerhebung.

.....

.....

.....

6. Nehmen Sie zu den Cartoons Stellung. Wie viel Wahrheit steckt dahinter?



Cartoon 1



Cartoon 2

.....

.....

.....

.....

7. Formulieren Sie ein Beispiel, das den Grundsatz der Zweckbestimmung bei der Datenverarbeitung verdeutlicht.

.....

.....

Trainingsaufgaben

- Wie lautet § 1 des Bundesdatenschutzgesetzes?
- Nennen Sie vier Beispiele für den Missbrauch persönlicher Daten.
- Definieren Sie den Begriff „personenbezogene Daten“.
- Nennen Sie drei Beispiele für personenbezogene Daten.
- Was bedeutet „Zweckbestimmung bei der Datenverwendung“?
- Nennen Sie fünf Arbeitnehmerdaten, die der Arbeitgeber in jedem Fall erfassen und speichern darf.
- Zählen Sie vier Maßnahmen auf, die im Unternehmen eine Voraussetzung für die Verarbeitung personenbezogener Daten darstellen.
- Nennen Sie drei Aufgaben eines betrieblichen Datenschutzbeauftragten.
- Unter welcher Voraussetzung ist die Ernennung eines betrieblichen Datenschutzbeauftragten erforderlich?

[Information]

[Training]



Training – Datenschutz und Datensicherheit, Kap. 1.5 bis 1.7

Einstiegssituation: Sicherheit beim Onlinebanking

Die Schöner Wohnen GmbH erhält die abgebildete E-Mail, die an Herrn Hans-Peter Göbel, den Leiter des Rechnungswesens, weitergeleitet wird. Soll Herr Göbel dem Link in der E-Mail folgen und auf der sich öffnenden Internetseite die Logindaten „Konto-Nr“, „Unterkonto-Nr“, „PIN“, „TAN 1“ und „TAN 2“ eingeben?

Von: Ferdinand Sorge [mailto: technischer_support@deutsche-bank.de]

Gesendet: Freitag, 6. Januar 20.. 16:02

An: Schöner Wohnen GmbH info@schoener-wohnen-wvd.de

Betreff: Bestätigung Ihrer Kundendaten

Deutsche Bank AG
Königstraße 7–11
47051 Duisburg

Sehr geehrte Damen und Herren,

unser technischer Support führt aktuell eine wichtige Softwareaktualisierung mit dem Ziel durch, die Qualität und die Sicherheit des Online-Banking-Systems zu optimieren.

Damit Sie diesen Service auch weiterhin für die „Schöner Wohnen GmbH“ nutzen können, ist eine Bestätigung Ihrer Kundendaten innerhalb von fünf Tagen erforderlich. Andernfalls sehen wir uns aus Sicherheitsgründen gezwungen, Ihr Konto zu sperren.

Wir bitten Sie, den folgenden Link anzuklicken, Ihre Kundendaten einzugeben und nach erfolgter Eingabe zu bestätigen.

<https://banking.deutsche-bank.de/>

Mögliche Unannehmlichkeiten bitten wir vorab zu entschuldigen und bedanken uns ganz herzlich für Ihre Mithilfe.

Ihre Deutsche Bank AG
Technischer Support
i. A. Ferdinand Sorge

1. Woran kann man erkennen, ob eine E-Mail bzw. eine Website möglicherweise gefälscht ist?
2. Führen Sie eine Internet-Recherche zum Begriff „Phishing“ durch und klären Sie, was Phishing ist und wie es funktioniert.
3. Welche Folgen könnte ein Login auf einer gefälschten Website (wie im Beispiel) haben?