

Datenschutz im Überblick

© Gesellschaft für

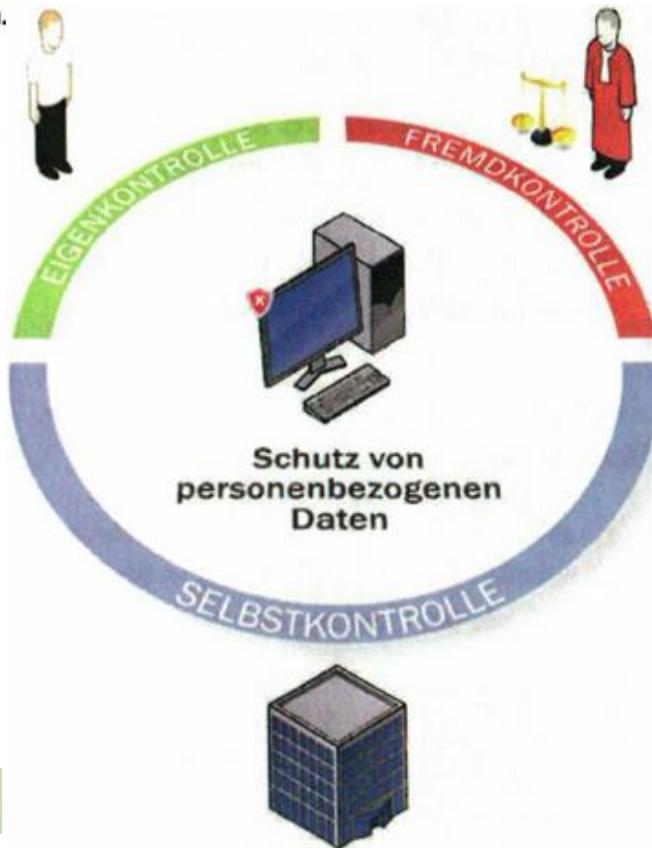
Datenschutz und Datensicherheit e.V. GDD für die Schule aufbereitet von J. Rau 2018



Der Betroffene ...

... übt seine Rechte aus

Der Betroffene kann Auskunft über gespeicherte Daten beantragen und ggf. Berichtigung, Löschung oder Sperrung erwirken.



Der Staat ...

... kontrolliert die Einhaltung

Die Datenschutz-Aufsichtsbehörde kann unzulässige Verfahren beanstanden, Bußgelder verhängen und Strafanträge stellen.

Das Unternehmen ...

... hat die Verantwortung

Das Unternehmen darf personenbezogene Daten nur dem Datenschutzrecht entsprechend erheben, verarbeiten und nutzen.

... organisiert den Datenschutz

Das Unternehmen macht die Vorgaben, wie und unter welchen Voraussetzungen personenbezogene Daten erhoben und verarbeitet werden dürfen.

... sichert die Daten

Personenbezogene Daten müssen vor unbefugtem Zugriff, Verlust und Zerstörung ausreichend geschützt werden.

Die Kontrollfunktion des Staates

Warum ist Datenschutz notwendig?

S

§ 1 Abs. 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.“

Die fortschreitende technische Entwicklung in der automatisierten Datenverarbeitung führt zu steigenden Gefahren des Datenmissbrauchs. Es fallen immer mehr Daten an, die nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können. Der Einzelne wird dadurch in seinen Persönlichkeits- und Freiheitsrechten beeinträchtigt, insbesondere wenn er nicht weiß, wer welche Daten über ihn hat, was dieser mit diesen macht und an wen er sie weitergibt. Deshalb bedarf jede personenbezogene Datenverarbeitung einer gesetzlichen Grundlage.

Die Grundlagen des Datenschutzes sind durch das Bundesdatenschutzgesetz (BDSG) geregelt. Daneben gibt es bereichsspezifische Vorschriften.

i

Daten über juristische Personen, Personenvereinigungen, Vereine, Verbände usw. werden nicht vom BDSG geschützt. Es gilt auch nicht für ausschließlich persönliche oder familiäre Tätigkeiten.

Wen schützt das BDSG?

Das BDSG schützt natürliche Personen bei der Verwendung ihrer personenbezogenen Daten. Geschützt sind demnach Mitarbeiter, Kunden und Lieferanten oder deren Ansprechpartner.

Wer muss das BDSG beachten?

1. Privatrechtliche Organisationen und Firmen, aber auch Personen, die personenbezogene Daten als Hilfsmittel für ihre eigenen Zwecke verarbeiten, z.B. Selbstständige, Vereine, Produktions-, Handels- und Dienstleistungsunternehmen.
2. Sonstige privatwirtschaftliche Organisationen, deren Geschäftszweck die Verarbeitung personenbezogener Daten für Fremde ist, wie Service-Rechenzentren, Wirtschaftsauskunfteien, Markt- und Meinungsforscher, Adressenhändler, -broker und -verlage sowie wissenschaftliche Forschungseinrichtungen und Medien.
3. Öffentliche Stellen des Bundes, z.B. die Bundesbehörden.

Kontrolle durch Datenschutzbehörden

§ 43 BDSG

Unbefugte Datenerhebungen und -verarbeitungen können mit einem Bußgeld bis zu 300.000 € und Gewinnabschöpfung, sonstige Verstöße mit Bußgeldern bis zu 50.000 € sanktioniert werden.

§ 44 BDSG

Strafrechtlich relevante Verstöße gegen den Datenschutz werden mit Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe bestraft.



Die Aufsichtsbehörde wird – nicht nur – bei Verdachtsfällen tätig: Sie hat Informations-, Betretens-, Besichtigungs-, Prüfungs- und Einsichtsrechte. Die Aufsichtsbehörde prüft die Zulässigkeit der Datenverarbeitung der Unternehmen, macht Auflagen zur Datensicherheit und kann unter Umständen sogar ein unzulässiges Verfahren untersagen. Zudem kann die Aufsichtsbehörde Bußgelder verhängen und Strafanträge stellen.

Konsequenzen von Datenschutzverstößen

Ordnungswidrigkeiten

sind bestimmte vorsätzliche oder fahrlässige Datenschutzverstöße. Dabei handelt es sich im Wesentlichen um Verstöße gegen Melde-, Dokumentations- oder Informationspflichten sowie um bestimmte unbefugte Datenerhebungs- oder Verarbeitungsschritte.

Straftaten

sind vorsätzliche Handlungen, die gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht begangen werden. Antragsberechtigt ist nicht nur der Betroffene, sondern auch die Datenschutz-Aufsichtsbehörde und das Unternehmen.

Schadensersatzpflichten

für das Unternehmen entstehen, wenn ein Betroffener durch unzulässige oder unrichtige Datenerhebung, Verarbeitung oder Nutzung einen nachweisbaren Schaden erleidet. Die Firma kann sich durch den Nachweis der gebotenen Sorgfalt davon befreien. Daneben kann unter Umständen auch der verantwortliche Mitarbeiter haftbar gemacht werden.

Arbeitsrechtliche Konsequenzen

Verstöße gegen den Datenschutz können für die Mitarbeiter auch arbeitsrechtliche Konsequenzen von der Abmahnung bis zur Kündigung haben.

Die Verantwortung des Unternehmens



§ 5 BDSG: Datengeheimnis

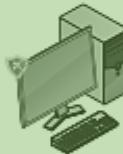
„Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“

Das Unternehmen hat die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung. Das BDSG spricht deshalb von der „verantwortlichen Stelle“. Dienstleister, die lediglich Datenverarbeitung im Auftrag betreiben (z.B. Service-Rechenzentren, Entsorger) werden der verantwortlichen Stelle zugeordnet. Das Unternehmen handelt über seine Leitung, also den Vorstand oder die Geschäftsführung.

Adressat des BDSG sind aber auch die einzelnen Mitarbeiter. Sie dürfen nicht unbefugt Daten erheben, verarbeiten oder nutzen. Deshalb ist das Unternehmen verpflichtet, die mit der Datenverarbeitung betrauten Personen mit den Vorschriften des BDSG und gegebenenfalls mit weiteren relevanten Datenschutzvorschriften vertraut zu machen. Darüber hinaus sind sie vor Beginn ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Wann müssen Unternehmen das BDSG beachten?

Das BDSG greift überall dort, wo personenbezogene Daten verarbeitet werden – sowohl auf EDV-Anlagen als auch in strukturierten Datensammlungen wie z.B. Karteikarten oder Akten.



Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.



Personenbezogene Daten
z.B. Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, Vermögen, Besitz, Arbeitsverhalten, Arbeitsergebnisse, Personalnummer, PC-Benutzerkennung, maschinenbezogene Nutzungszeiten

Besonders sensible Daten
z.B. rassistische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben

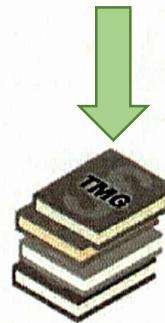
Das betrifft die Daten von Mitarbeitern und Kollegen genauso wie die von Kunden oder Lieferanten. Auch Daten ohne direkten Personenbezug (z.B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen geschlossen werden kann (z.B. Personalnummer, KFZ-Kennzeichen). Der Schutzbedarf von Daten hängt von ihrem Verwendungszusammenhang ab. Dennoch gibt es nach dem BDSG „besonders sensible Daten“. Ihre Verarbeitung ist nur unter strengen Regeln erlaubt, ihre Verwendung für Marketingzwecke in der Regel unzulässig.

Wann ist die Datenverarbeitung zulässig?

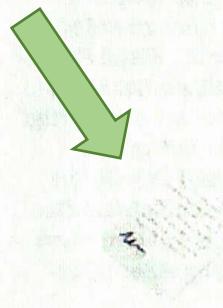
Jede Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten bedarf einer gesetzlichen Rechtfertigung. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.



oder



oder



Erlaubnis durch das BDSG

Das BDSG erlaubt die Verarbeitung personenbezogener Daten,

- wenn sie dem Zweck des Vertrags oder der Vertragsanbahnung mit dem Betroffenen dient.
- wenn die berechtigten Interessen des Unternehmens die schutzwürdigen Interessen des Betroffenen am Ausschluss der Verarbeitung überwiegen.
- wenn die Daten allgemein zugänglich sind oder aufgrund ihres Charakters veröffentlicht werden dürften.

Erlaubnis durch andere Rechtsvorschriften

Auch außerhalb des BDSG gibt es Rechtsvorschriften, die es gestatten oder sogar dazu verpflichten können, Daten zu verarbeiten. Von hoher praktischer Relevanz sind beispielsweise das Steuer- und Sozialversicherungsrecht für die Entgeltabrechnung oder das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) für Telekommunikations- und Internetanbieter. Für die Verarbeitung von Personaldaten sind abgeschlossene Betriebs- oder Dienstvereinbarungen vorrangig.

Einwilligung des Betroffenen

Die Datenverarbeitung ist erlaubt, wenn der Betroffene darin einwilligt. Die Einwilligung muss sich auf die konkreten Verarbeitungsvorgänge beziehen und regelmäßig schriftlich erklärt werden.

Formen des Umgangs mit personenbezogenen Daten



Löschen

Unkenntlichmachen durch physikalische Vernichtung (z.B. Aktenvernichter) oder durch das Entfernen der Daten vom Datenträger (z.B. Überschreiben von Festplatten).



Erheben

Datenbeschaffung beim Betroffenen selbst (z.B. durch schriftliche oder mündliche Befragung) oder bei Dritten (z.B. Kauf von Adressen bei einem Adresshändler).



Speichern

Erfassen und Aufbewahren auf einem Datenträger.



Verändern

Inhaltliches Umgestalten, in einen neuen Kontext stellen.



Nutzen

Jede andere Art der Verwendung, wie z.B. Auswertungen.



Sperren

Kennzeichnung, um die weitere Verarbeitung einzuschränken (z.B. bei Werbewiderspruch).



Weitergeben

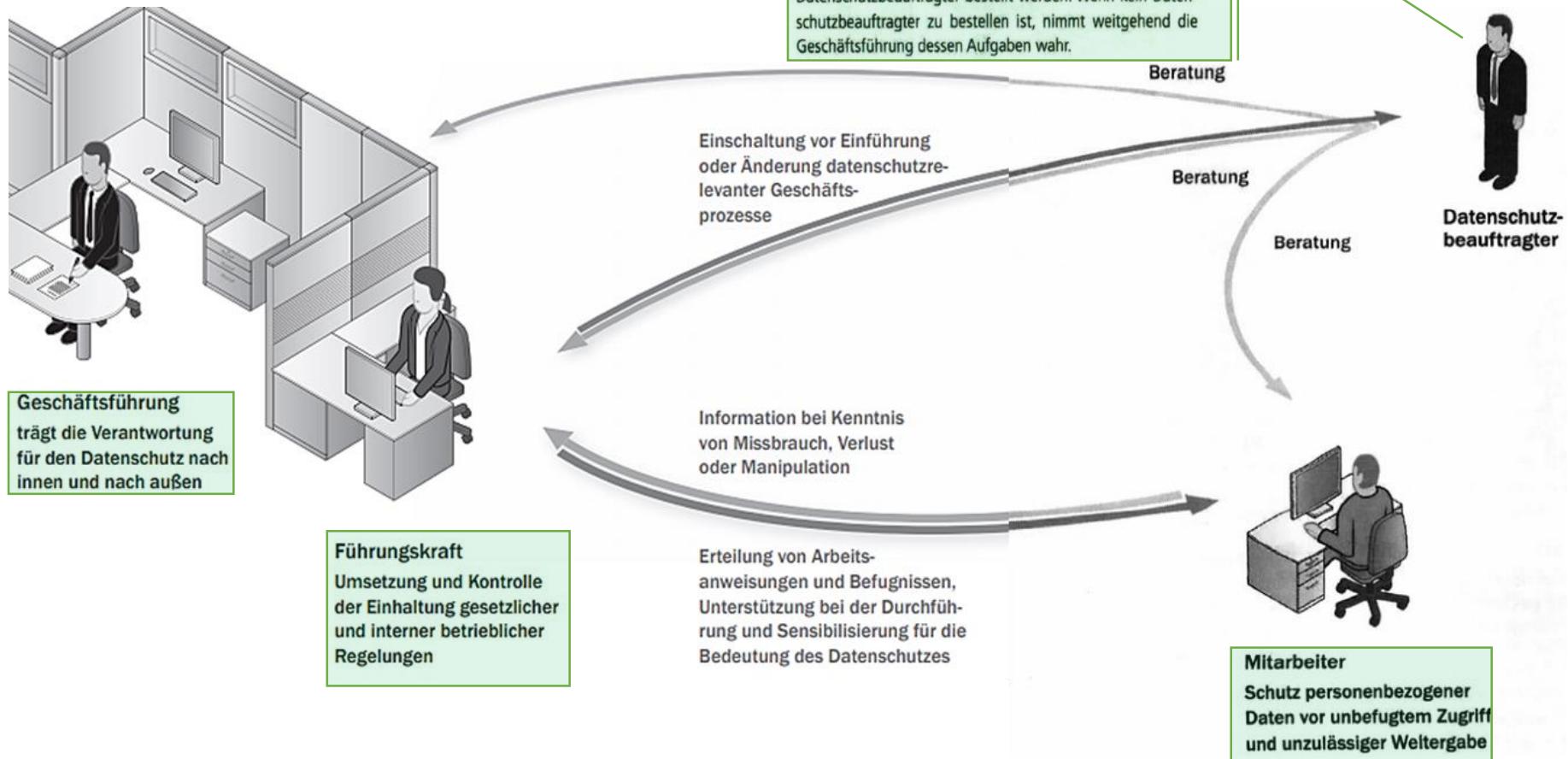
Transfer an Personen derselben verantwortlichen Stelle (Firma, Organisation).



Übermitteln

Weitergabe an Personen außerhalb der eigenen Firma oder Organisation (Dritte).

Alle im Unternehmen tragen Verantwortung



Zulässig oder nicht? (mit Begründung)



Ein Unternehmen speichert seine Kundendaten zur Abwicklung eines Kaufvertrages und zur Prüfung möglicher Gewährleistungsansprüche.

Nutzung von Daten für eigene Werbezwecke, obwohl der Kunde erklärt hat, keine Werbung erhalten zu wollen.

Ein Unternehmen verschickt Mailings per Post an seinen bestehenden Kundenstamm, um ein neu eingeführtes Produkt zu bewerben.

Ein Unternehmen übermittelt die Lohn- und Einkommensdaten seiner Mitarbeiter an das Finanzamt und an die Sozialversicherungsträger.

Ein Arzt gibt die Adressdaten seiner Patienten an einen Arzneimittelhersteller weiter, damit dieser gezielt seine Medikamente bewerben kann.

Ein Unternehmen regelt in einer Betriebsvereinbarung die Erfassung der Arbeitszeit und die Nutzung der anfallenden Daten zur Abrechnung von Gehalt, Urlaub und Überstunden.

Ein Unternehmen veröffentlicht das Foto eines Vertriebsmitarbeiters auf seiner Internetseite.

Ein Unternehmen beabsichtigt, seine Kunden (Verbraucher) telefonisch auf seine neuen Produkte hinzuweisen.

Maßnahmen zur Datensicherheit

Datensicherheitsmaßnahmen sind notwendig, um den Datenschutz abzusichern.

Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren, z.B. durch Festlegung der befugten Personen, Ausweisleser, Abschließen der Räume.



Verfügbarkeitskontrolle

Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust (z.B. durch Wasserschäden, Blitzschlag, Stromausfall) geschützt sein, z.B. durch das Erstellen von Sicherungskopien, die an besonders geschützten Orten gelagert werden.

Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, z.B. durch Verwendung von Passwörtern.



Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, in diesen verändert oder aus diesen entfernt worden sind, z.B. durch Protokollierung.



Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, z.B. durch Einschließen der Datenträger, Lagerung in einem Sicherheitsbereich, Regelungen für die sichere Vernichtung nicht mehr benötigter Datenträger.



9 BSG

Gebot der Datentrennung

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.

Auftragskontrolle

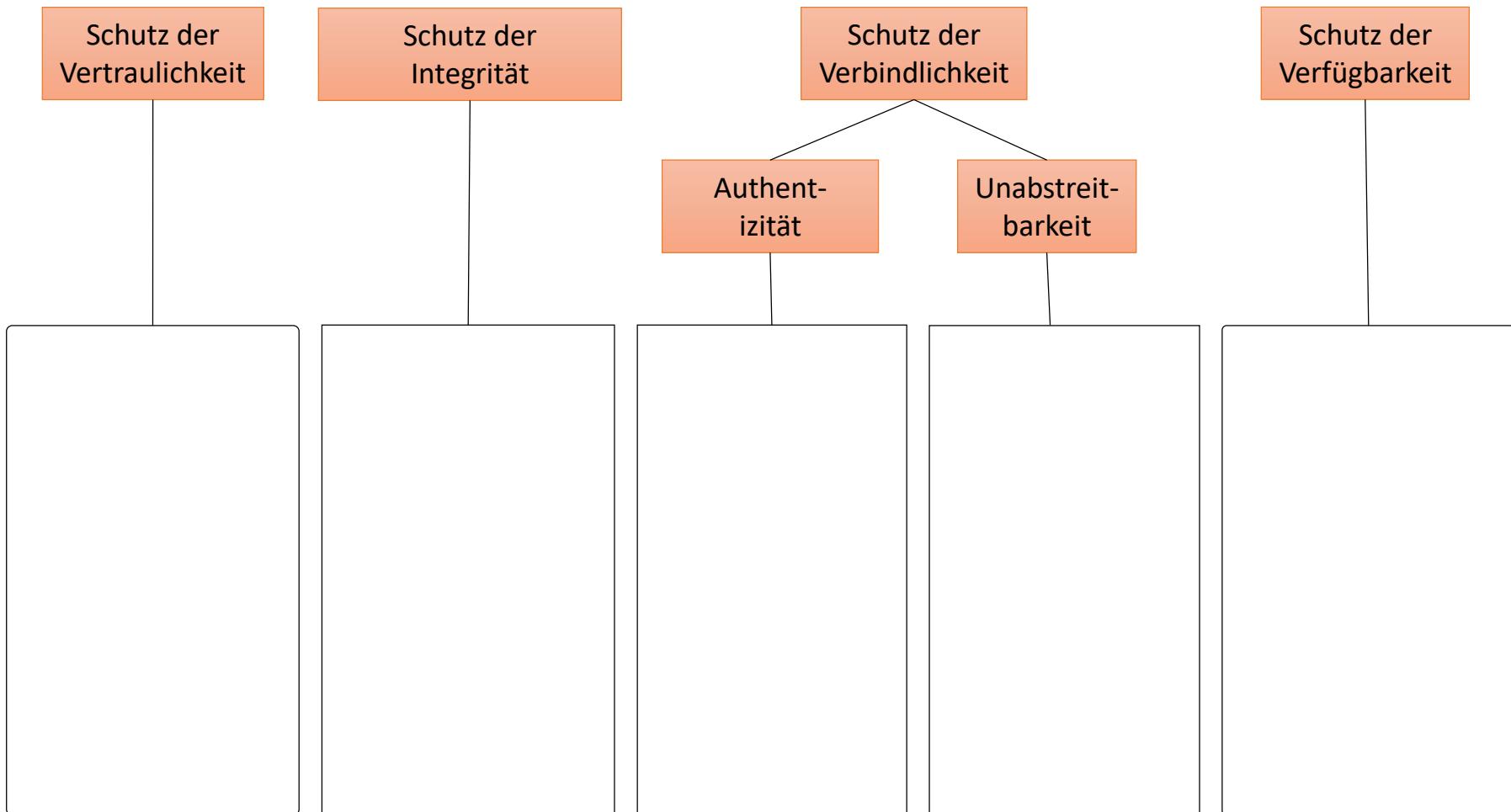
Es ist sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist, z.B. durch Verschlüsselung der Daten, Transport der Datenträger in verschlossenen Behältnissen.

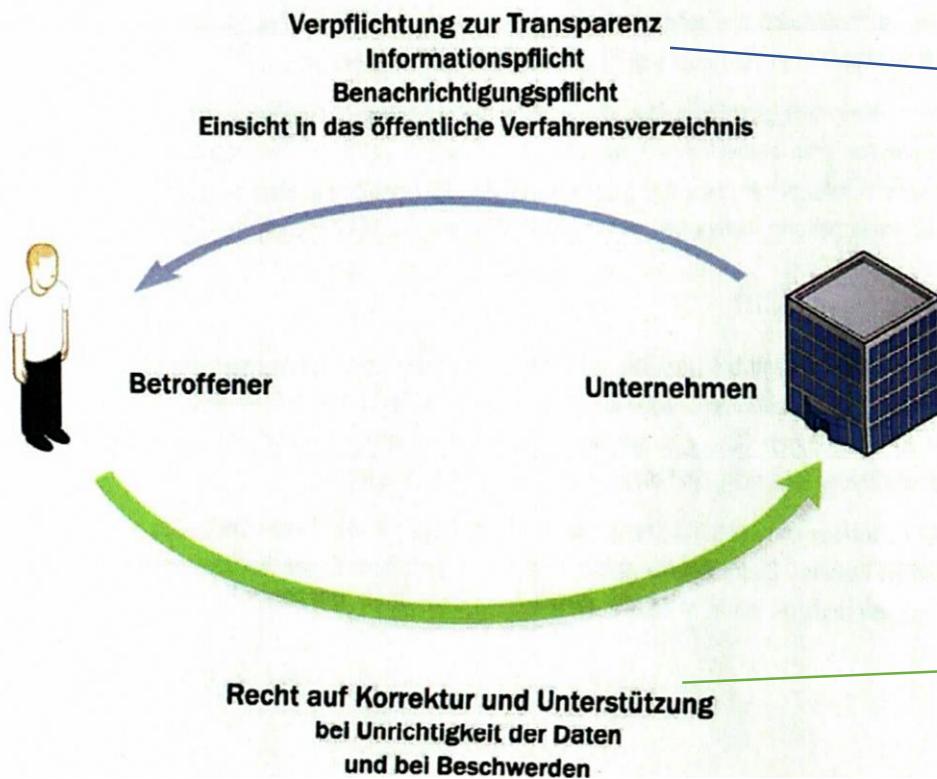
Das BDSG verlangt zur Gewährleistung des Datenschutzes die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen. Diese Maßnahmen werden auch als die 8 Gebote der Datensicherheit bezeichnet.

Ordne die Maßnahmen zur Datensicherheit in das Schema ein.



Rechte der Betroffenen

Diejenige natürliche Person, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekt des Gesetzes sind, bezeichnet das BDSG als „Betroffener“. Betroffene können beispielsweise der Mitarbeiter, der Kunde, oder der Ansprechpartner eines Firmenkunden sein. Den Betroffenen räumt das BDSG Transparenz-, Korrektur- und Unterstützungsrechte ein.



Transparenzpflicht

Die verantwortliche Stelle hat eine *Informationspflicht* gegenüber dem Betroffenen. Sie muss ihm bei der Erhebung seiner personenbezogenen Daten ihre Identität, den Zweck der Erhebung, Verarbeitung oder Nutzung dieser Daten sowie mögliche Kategorien von Empfängern mitteilen. Werden die Daten bei Dritten erhoben (z.B. bei Auskunfteien oder Adresshändlern), besteht eine *Benachrichtigungspflicht*, die jedoch mit einem umfangreichen Ausnahmekatalog versehen ist.

Falls der Betroffene anfragt, ist die verantwortliche Stelle zur *Auskunft* über die gespeicherten Daten, deren Herkunft und mögliche Empfänger sowie über den Zweck der Speicherung verpflichtet. Die Auskunft ist in der Regel schriftlich und unentgeltlich zu erteilen.

Ferner kann sich jedermann über die ihn eventuell betreffende Datenverarbeitung durch Einsicht in das von dem betrieblichen Datenschutzbeauftragten geführte *Öffentliche Verfahrensverzeichnis* informieren. Es enthält einen Überblick über betroffene Personengruppen, Zwecke der Datenverarbeitung, Kategorien von Datenempfängern und Löschfristen.

Korrekturrecht

Der Betroffene kann bei Unrichtigkeit die Korrektur oder bei Unzulässigkeit der Verarbeitung die Löschung seiner personenbezogenen Daten verlangen. Bei strittigen Sachverhalten sind die Daten bis zur endgültigen Klärung zu sperren. Falls der Betroffene der Verwendung seiner Daten zu Werbezwecken widerspricht, sind diese hierfür ebenfalls zu sperren.

Der Betroffene kann sich mit Beschwerden oder Anfragen an den betrieblichen Datenschutzbeauftragten wenden. Dieser unterliegt hinsichtlich des Betroffenen einer Verschwiegenheitsverpflichtung, sofern dieser ihn nicht davon befreit hat.

- 1** Das BDSG schützt ...
- a) Unternehmen
b) natürliche Personen
-
- 2** Die Datenschutzaufsichtsbehörde kann ...
- a) Mitarbeiter kündigen
b) Bußgelder verhängen
-
- 3** Die Verantwortung für den Datenschutz im Unternehmen hat ...
- a) der Geschäftsführer/Vorstand
b) die Führungskraft
c) der Mitarbeiter
-
- 4** Die Nutzung von eigenen Kundenstammdaten zu Werbezwecken für eigene Produkte ist grundsätzlich ...
- a) zulässig
b) unzulässig
-
- 5** Daten, die nicht mehr benötigt werden, sind ...
- a) zu löschen
b) zu sperren
-
- 6** Die Zugangskontrolle kann unter anderem erreicht werden durch ...
- a) Abschließen von Räumen
b) Passwortschutz
-
- 7** Die Datenschutzkontrolle wird ausgeübt durch ...
- a) die Mitarbeitervertretung
b) die Aufsichtsbehörde
c) den betrieblichen Datenschutzbeauftragten
-
- 8** Falls der Betroffene keine Werbung wünscht, kann er verlangen, die Daten ...
- a) zu löschen
b) zu sperren
-
- 9** Die Verpflichtung zur Wahrung des Datengeheimnisses verlangt ...
- a) das Unterlassen unbefugter Datenverarbeitung
b) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses
-

