

Software-Projekt I

Prof. Dr. Rainer Koschke

Arbeitsgruppe Softwaretechnik
Fachbereich Mathematik und Informatik
Universität Bremen

Sommersemester 2014

Rechtlicher Rahmen der Softwareentwicklung I

Rechtlicher Rahmen

- Datenschutzgesetz
- Betriebsverfassungsgesetz
- Arbeitsschutzgesetz
- Bildschirmarbeitsverordnung
- Normen und Richtlinien
- Telemediendienste

Rechtlicher Rahmen der Software-Entwicklung

- Datenschutzgesetz
- Betriebsverfassungsgesetz
- Arbeitsschutzgesetz
- Bildschirmarbeitsverordnung
- Normen (DIN, EN, ISO), Richtlinien (VDI)
- Tele- und Mediendienste –
Rechtsgrundlagen

Grundsätze des Volkszählungsurteils 1983

Recht auf informationelle Selbstbestimmung

*Unter den Bedingungen der modernen Datenverarbeitung wird der **Schutz des Einzelnen** gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe **seiner persönlichen Daten** von dem allgemeinen **Persönlichkeitsrecht** des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, **grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen** (BVerfGE 65, 1).*

5 / 56

Definition

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

§3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG)

6 / 56

Wörtliches Zitat aus der Quelle https://de.wikipedia.org/wiki/Personenbezogene_Daten:

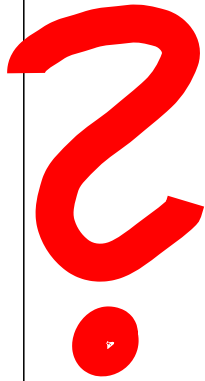
Personenbezogene Daten sind laut §3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“. Die entsprechenden landesgesetzlichen Definitionen haben den gleichen oder einen ähnlichen Wortlaut.

Besonders schutzbedürftig sind nach §3 Abs. 9 des BDSG „besondere Arten personenbezogener Daten“. Hierzu zählen Gesundheitsdaten, Informationen über die rassische oder ethnische Herkunft, politische, religiöse, gewerkschaftliche oder sexuelle Orientierung. Ihre Verarbeitung ist an strengere Voraussetzungen gebunden als die Verarbeitung sonstiger personenbezogener Daten.

Grundsätze des Volkszählungsurteils 1983

Das Recht auf informationelle Selbstbestimmung darf nur unter folgenden Bedingungen eingeschränkt werden (BVerfGE 65, 1):

- Normenklarheit
- Verhältnismäßigkeit
- Zweckbindung
- Pflicht zu organisatorischen und verfahrensrechtlichen Vorkehrungen



- Welche Arten von personenbezogenen Daten fallen im Bibliotheksbetrieb an?
- Unter welchen Umständen dürfen personenbezogene Daten in der Bibliothek erhoben werden?
- Wie lange dürfen diese Daten aufbewahrt werden?

8 / 56

Definition

Bestandsdaten: Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Tele-, Medien- und Telekommunikationsdiensten.

Beispiele: Name, Anschrift, E-Mail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, aber auch statische IP-Adressen.

Definition

Nutzungsdaten Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Teledienste.

9 / 56

Wir unterscheiden zwischen personenbezogenen Bestands- und Nutzungsdaten.

Zum Umgang dieser personenbezogenen Daten bei Internetdiensten zitiert von
http://www.datenschutz.hessen.de/_old_content/tb31/k25p03.htm:

Bestandsdaten sind Daten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Tele-, Medien- und Telekommunikationsdiensten. Dies können sein: Name, Anschrift, E-Mail-Adresse, Telefon- oder Telefaxnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel, User-ID, aber auch statische IP-Adressen und ähnliche Angaben.

- Welche Bestandsdaten dürfen erhoben werden?
In welchem Umfang Bestandsdaten erhoben werden, ist am Grundsatz der Erforderlichkeit auszurichten, d.h., Daten, die für die genannten Zwecke nicht zwingend erforderlich sind, dürfen nicht erhoben, verarbeitet oder genutzt werden.
- Wann müssen sie gelöscht werden?
Erforderlichkeitsgrundsatz: Soweit Bestandsdaten nicht mehr zur Begründung, Ausgestaltung und Änderung des Vertragsverhältnisses erforderlich sind, etwa weil das Vertragsverhältnis beendet ist und nachvertragliche Ansprüche nicht mehr bestehen, müssen sie frühestmöglich gelöscht werden.

Nutzungsdaten Nutzungsdaten sind gem. §6 Abs. 1 TDDSG beziehungsweise §19 Abs. 2 MDStV Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und diese abzurechnen. Es handelt sich hierbei insbesondere um Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die von den Nutzenden in Anspruch genommenen Teledienste. Sie fallen im Regelfall bei jedem Tele- und Mediendiensteanbieter an

Die Regelungen sind abschließend, d.h. die Erhebung, Verarbeitung oder Nutzung der Nutzungs- und Abrechnungsdaten durch die Diensteanbieter ist nur zulässig, soweit sie durch die Vorschriften erlaubt wird. Nutzungsdaten dürfen außerhalb dieser Bestimmungen nur verarbeitet werden, wenn eine gesetzliche Spezialregelung dies ausdrücklich erlaubt oder der Betroffene eingewilligt hat.

Die Aussagekraft der Nutzungsdaten bei Tele- und Mediendiensten ist bisweilen größer als etwa bei Verbindungsdaten der Sprachtelekommunikation. Während Verbindungsdaten lediglich Auskunft darüber geben, wer wann mit wem kommuniziert hat, offenbaren Nutzungsdaten häufig darüber hinaus, welche Inhalte übertragen wurden. Dies gilt insbesondere in Bezug auf aus dem Web abgerufene Ressourcen und auf Anfragen bei Suchmaschinen.

Löschungsfristen von Nutzungsdaten: Nach §6 Abs. 4 TDDSG darf der Diensteanbieter Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung erforderlich sind. Im Umkehrschluss bedeutet dies, dass alle übrigen Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der Nutzung zu löschen sind. Eine entsprechende Regelung liefert §19 Abs. 5 MDStV.

Grundsätzliche Regeln

- Betroffene aufklären, welche Daten wofür benutzt werden und wie lange sie gespeichert werden.
- Verhältnismäßigkeit und Zweckbindung beachten
- Einwilligung der Betroffenen einholen
- Auskunftsrecht der Betroffenen, wie mit ihren Daten umgegangen wird, beachten
- vertragliche und vertragsähnliche Zwecke können Datenverwendung durch das Gesetz erlauben
- Erforderlichkeit nachweisen
- nicht mehr erforderliche Daten frühestmöglich löschen

10 / 56

Siehe auch die Hinweise (Zitat) zur Rechtfertigung der Erhebung personenbezogener Daten unter http://www.bwr-media.de/datenschutz/5655_bundesdatenschutzgesetz-wann-sie-personenbezogene-daten-erheben-speichern-und-nutzen-duerfen/:

Grundsätzlich ist Ihnen verboten, was nicht ausdrücklich erlaubt wurde. Das bedeutet, im BDSG gilt als allgemeiner Grundsatz: Ein Verbot mit Erlaubnisvorbehalt zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

Sie dürfen also keine Daten erheben, verarbeiten und nutzen. Ausnahme: Der Betroffene hat dazu ausdrücklich seine Einwilligung erklärt oder eine andere gesetzliche Vorschrift rechtfertigt den Vorgang.

Im Übrigen müssen die Betroffenen bei Ihrer Einwilligung ausreichend informiert werden. Und sie müssen diese Einwilligung in die Datenverarbeitung freiwillig und schriftlich erteilen. So müssen Sie den Betroffenen zum Beispiel über den Zweck der Erhebung oder die Nutzung seiner personenbezogenen Daten aufklären.

Achten Sie darauf, dass die Einwilligung vor der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten vorliegt.

Jeder Betroffene hat ein Auskunftsrecht darüber, wie mit seinen Personendaten umgegangen wird – also über Art, Umfang, Zweck und Nutzung.

Grundsätzlich gilt, dass Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten immer dann zulässig sind, wenn ein Gesetz dies erlaubt (für Unternehmen vor allem §28 BDSG) oder wenn der Betroffene eingewilligt hat, §4 Abs. 1 BDSG.

Zur Vereinfachung wird in den nachfolgenden Ausführungen für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Begriff „Verwendung“ benutzt.

Erlaubnis der Datenverwendung durch das Gesetz

- Vertragliche und vertragsähnliche Zwecke (§28 Absatz 1 Satz 1 Ziffer 1 BDSG)
Diese Norm erlaubt die Datenverwendung zu vertraglichen oder vertragsähnlichen Zwecken. Zwischen Datenverarbeitung und dem Vertragszweck muss ein unmittelbarer Zusammenhang bestehen. Sie muss erfolgen, um vertragliche Pflichten zu erfüllen. Gleiches gilt für die Verwendung zu vertragsähnlichen Zwecken.
Beispiel: Die Anlieferung eines Fernsehgerätes an einen Kunden ist ohne Kenntnis seines Namens und seiner Wohnanschrift nicht möglich (§28 Absatz 1, Satz 1, Ziffer 1 BDSG).
Ebenso verhält es sich mit der Übermittlung von Daten – zur Erfüllung des Vertragszweckes – an Dritte.
Beispiel: Ein Kunde bucht in einem Reisebüro eine Reise. Seine Daten dürfen dann, auch wenn sich im Reisevertrag dazu keine ausdrückliche Regelung findet, entsprechend dem Umfang des Vertrages für die Buchung des Fluges, des Hotels usw. verwendet werden. Das heißt, das Reisebüro darf die Daten des Kunden, soweit dies für die Durchführung des Reisevertrages nötig ist, erheben, speichern und übermitteln. Andernfalls könnte das Reisebüro den Vertrag mit dem Kunden nicht erfüllen. Das Reisebüro muss allerdings z.B. die Fluggesellschaft darauf hinweisen, dass sie die Kundendaten nur zur Buchung eines bestimmten Fluges verwenden darf und insbesondere die Daten ihrerseits nicht (ohne vorherige schriftliche Einwilligung) außerhalb des Vertragszweckes weitergeben darf. Hintergrund ist wieder die Transparenzidee: Der Kunde muss wissen, wo seine Daten überall verwendet werden. Eine „Datenspeicherung auf Vorrat“ ist nicht zulässig, da auch in einem solchen Fall der Betroffene nicht erkennen kann, in welchem Umfang Daten von ihm zu welchem Zweck gespeichert oder sonst wie verwendet werden.
- Daten von Arbeitnehmern
Ob Unternehmen Daten von Arbeitnehmern verwenden dürfen, richtet sich ebenfalls nach §28 Absatz 1 Ziffer 1 BDSG.
Der Arbeitgeber darf Arbeitnehmerdaten, die für das Arbeitsverhältnis von grundlegender Bedeutung sind (sogenannter Zweckzusammenhang), verwenden. Dazu gehören u.a. Name, Alter, Beruf, sonstige Qualifikationen und Einsatzfähigkeit. Dazu gehören auch Arbeitnehmerdaten, die zwar zur Zeit noch nicht von Bedeutung sind, die es aber werden könnten. Nicht verwendet werden dürfen Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse (Ausnahme: Konfession für die Abführung von Kirchensteuern aufgrund gesetzlicher Regelungen) oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.
Bitte beachten Sie: Auch Bewerbungsmappen enthalten personenbezogene Daten. Falls Sie Bewerber in einem Einstellungsverfahren nicht berücksichtigen konnten, sind diese Daten zu löschen. Die Zweckbindung entfällt nach Beendigung des Einstellungsverfahrens. Liegen die Daten in Papierform vor, geben Sie diese zurück oder vernichten Sie die Unterlagen.
- Berechtigtes Interesse (§28 Abs.1 S. 1 Ziff 2 BDSG)
Bei Vorliegen eines berechtigten Interesses dürfen Unternehmen Daten dann verwenden, wenn davon ausgegangen werden kann, dass keine schutzwürdigen Belange des Betroffenen entgegenstehen. Das praktischste Beispiel ist das sogenannte „Outsourcing“, beispielsweise des Rechenzentrums. Dabei werden Daten, die bereits beim Betroffenen erhoben wurden, an eine Stelle außerhalb des Unternehmens übermittelt und dort gespeichert oder für Zwecke des Unternehmens genutzt. Entscheidend ist dabei, dass die Gesamtverantwortung für die Datenverarbeitung bei dem Unternehmen verbleibt.
- Allgemein zugängliche Quellen (§28 Abs.1 S. 1 Ziff. 3 BDSG)
Unternehmen dürfen auch Daten verwenden, die sie aus allgemein zugänglichen Quellen haben. Allgemein zugängliche Quellen sind u. a. Rundfunk- und Fernsehsendungen, Internet, Zeitschriften, Zeitungen und sonstige Publikationen, die von jedem gekauft werden können. Es ist also zum Beispiel erlaubt, die Anschrift eines Vertragspartners aus dem Telefonbuch heraus zu suchen und der eigenen Adresskartei beizufügen. Aufgrund der Öffentlichkeit von Verzeichnissen wie etwa dem Handelsregister, gilt dort Ähnliches. Nicht zu diesen Quellen zählen u. a. Grundbuch und Schuldnerverzeichnis. Denn derjenige, der in diese Register Einsicht nehmen will, muss ein berechtigtes Interesse daran haben.

- Der Erforderlichkeits-Maßstab

Maßstab für den Umgang mit Daten im Sinne von §28 BDSG ist immer die Erforderlichkeit der Datenverwendung. Diese ergibt sich aus einer Abwägung zwischen dem Interesse des Betroffenen an der Geheimhaltung und dem Interesse des Unternehmers an der Verwendung. Überwiegt das Interesse an der Datenverwendung gegenüber dem Interesse am Geheimnisschutz, kann der Anspruch auf Datenschutz eingeschränkt sein. Es gilt das Gebot der Datensparsamkeit. Danach dürfen nur so viele Daten wie unbedingt nötig verwendet werden.

Beispiel: Bei einer Gewinnspielkarte werden als Teilnehmerdaten Name, Vorname und die Anschrift erhoben. Diese Daten sind erforderlich, um den Gewinner zu ermitteln und ihm den Gewinn zu übersenden. Häufig wird auch die Angabe des Geburtsdatums verlangt, um festzustellen, ob der Teilnehmer geschäftsfähig ist. Auf die Freiwilligkeit und den Zweck dieser Datenerhebung ist hinzuweisen. Zur Erhebung zusätzlicher Daten mit Einwilligung des Betroffenen s.u., Ziffer 3.

Nachname	Koschke	Geburtsdatum	
Vorname	Rainer	Nutzertyp	Professor an der Universität Bremen
Akad. Titel	Prof. Dr.	Matrikelnummer	
Geschlecht	männlich	E-Mail	koschke@informatik.uni-bremen.de
	Meldeanschrift laut Personalausweis bzw. Pass mit Meldebestätigung		Weitere Anschrift
c/o		c/o	
Str. / Nr.		Str. / Nr.	
Zimmer		Zimmer	
PLZ / Ort		PLZ / Ort	
Telefon	0421/218-64481	Telefon	
Mobil		Mobil	

Benachrichtigungen per E-Mail

Ich bitte um elektronische Benachrichtigungen (z.B. Vormerkungen und Leihfristende) durch die Universitätsbibliothek an meine oben aufgeführte E-Mail-Adresse.

Wichtiger Hinweis

Die Angabe Ihrer Daten ist freiwillig. Ohne Ihre Daten ist eine Ausleihe jedoch nicht möglich. Die Erhebung der Daten erfolgt lediglich zum Zweck der automatisierten Ausleihverbuchung, der Online-Fernleihe sowie der Internet-Nutzung in den Räumen der Universitätsbibliothek. Die Daten werden nicht an Dritte weitergegeben. Grundlage für diese Datenerhebung ist das [Bremische Datenschutzgesetz \(BremDSG\)](#) vom 4. März 2003 (Brem. GBL. S.85), 10.

Bitte holen Sie ihren Bibliotheksausweis innerhalb von 30 Tagen ab. Danach werden die Daten gelöscht und müssten erneut eingegeben werden.

Erklärung

Die [Benutzungsordnung für die Staats- und Universitätsbibliothek Bremen](#) erkenne ich als verbindlich an. Im übrigen gilt die [Gebührenordnung](#).

Mit der Speicherung meiner personenbezogenen Daten

1. in der Universitätsbibliothek im Rahmen der Benutzung
2. in der Verbundzentrale des Gemeinsamen Bibliotheksverbundes (GBV) in Göttingen im Rahmen der Online-Fernleihe

bin ich einverstanden.

[Zurück](#)

[Anmeldung absenden](#)

[Abbrechen](#)

Auszug aus der Benutzungsordnung der Staats- und
Universitätsbibliothek Bremen als Beispiel¹:

§5 Verarbeitung von personenbezogenen Daten

- (1) Die Bibliothek verarbeitet personenbezogene Daten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Für das Nutzerverhältnis handelt es sich um folgende Daten:
 1. Benutzerstammdaten: Name und Anschrift(en), ggf. Telefonnummer, Geburtsdatum, Geschlecht, Benutzernummer und ggf. Matrikelnummer, Paßwort, Aufnahmedatum, ggf. Datum der letzten Änderung dieser Daten, Ablauf der Ausleihberechtigung, Benutzertyp (gibt die Zugehörigkeit zu einer bestimmten Benutzergruppe wieder) und Benutzerstatus (gibt die momentane Ausleihberechtigung wieder)
 2. Benutzungsdaten: Ausleihdatum, Leihfristende, Anzahl und Datum von Fristverlängerungen, Rückgabedatum, Vormerkungen und Bestellungen mit Datum, Entstehungsdatum und Betrag von Gebühren, Kosten und Auslagen, Sperrvermerk, Anzahl der gegenwärtigen Mahnungen
- (2) Die buchbezogenen Benutzungsdaten werden gelöscht, sobald der Benutzer das entsprechende Werk zurückgegeben und ggf. entstandene Gebühren, Kosten oder Auslagen bezahlt hat.
- (3) Die Benutzerstammdaten werden spätestens nach zweijähriger Inaktivität des Benutzers gelöscht, sofern er zu diesem Zeitpunkt alle Verpflichtungen gegenüber der Bibliothek erfüllt hat.

12 / 56

¹) [http:](http://www.suub.uni-bremen.de/uploads/cms/files/Benutzungsordnung.pdf)

Grundsätze des Volkszählungsurteils 1983

Normenklarheit :

- Gesetz muß klar verständlich sein;
- darf nicht zu unbestimmte Rechtsbegriffe (d.h. Begriffe, die nicht näher definiert und somit der Interpretation offen sind) oder Generalklauseln (die keine konkreten sachlichen Grenzen setzen) verwenden;
- für den Betroffenen muss klar erkennbar sein, warum konkret das Recht auf informationelle Selbstbestimmung eingeschränkt wird.

14 / 56

Weiterführender Links:

- Datenschutz am Fall (Vorlesung an der TU Berlin)::
<http://ig.cs.tu-berlin.de/oldstatic/w2000/ir1/t11-02/>
- Bremisches Datenschutzgesetz:
http://www.datenschutz-bremen.de/pdf/bremische_datenschutzgesetz.pdf

Grundsätze des Volkszählungsurteils 1983

Verhältnismäßigkeit und Zweckbindung:

Mittel müssen in einem rechten Verhältnis zu den Zwecken stehen, d.h.

- **Datensparsamkeit:** nur unbedingt notwendige Daten werden verarbeitet;
- **Zweckbindung:** Daten dürfen grundsätzlich nur für den Zweck benutzt werden.

15 / 56

Grundsätze des Volkszählungsurteils 1983

Organisatorische und verfahrensrechtliche Vorkehrungen:

- **Datensicherheit:** Daten können nicht manipuliert werden etc.,
- **Transparenzgebot:** Datenverarbeitung muss organisatorisch auch so ablaufen, dass externe Stellen – z.B. ein Datenschutzbeauftragter – kontrollieren können, ob alles „mit rechten Dingen zugeht“.

16 / 56

Datenschutz versus Datensicherheit

Datenschutz:

Ziel: Beeinträchtigung schutzwürdiger Belange der Betroffenen, deren Daten erhoben sind oder werden sollen, entgegenzuwirken (BDSG 1978).

Datensicherheit (IT-Security)

Ziel: Schutz vor Verfälschung und Verlust von Daten und vor unberechtigten Zugriffen auf Daten.

17 / 56

Datenschutz:

Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken (BDSG 1978).

Datensicherheit

ist die Menge der Maßnahmen zum Schutz des Betreibers (Anwenders) im Hinblick auf die Funktionsfähigkeit von DV-Systemen, insbes. zum Schutz vor Verfälschung und Verlust von Daten und vor unberechtigten Zugriffen auf Daten (International: IT-Security)

Datensicherung ist der technische Vorgang des Speicherns einer Sicherungskopie.

Datenschutz versus Datensicherheit

Datenschutz

↔ Datensicherheit

Gemeinsamkeiten:

Technisch-organisatorische Maßnahmen

Vertraulichkeit als Teilziel

Unterschiede:

nur personenbezogene Daten	↔	alle Daten
Erhebung, Speicherung, Verarbeitung und Nutzung	↔	Speicherung, Verarbeitung und Nutzung
Rechtliche Normen	↔	Technische Normen
Gebot der Datensparsamkeit	↔	Tendenz zur Redundanz

18 / 56

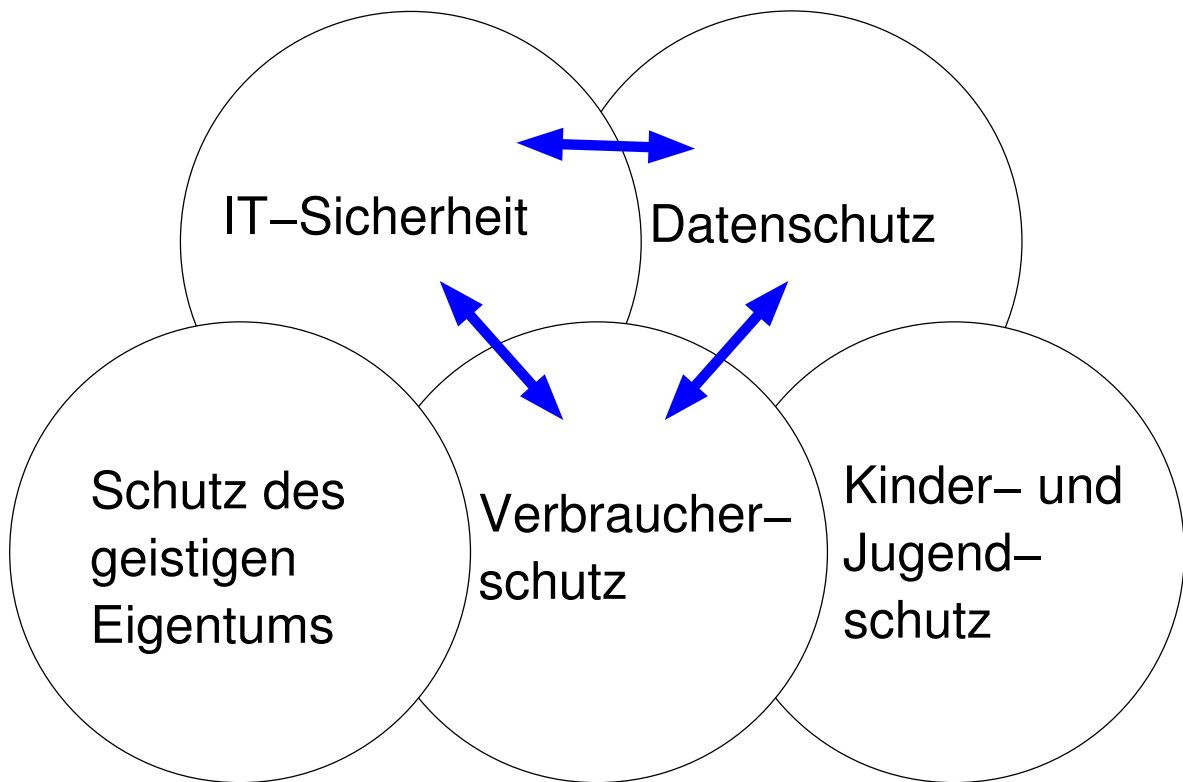
Allgemeine Sicherheitsanforderungen/Kriterien

ITSEC, ISO 7498-2:

- Vertraulichkeit: Schutz vor unbefugter Preisgabe von Informationen
- Verfügbarkeit: Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln
- Integrität: Schutz vor unbefugter Veränderung von Informationen, Programmen, des Systems oder Netzwerkes

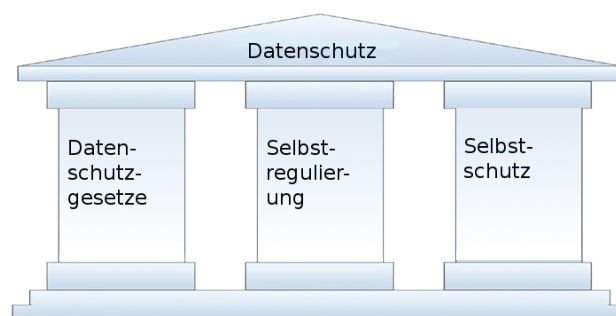
19 / 56

Weitere Schutzbereiche - zum Teil in Konflikt mit dem Datenschutz



20 / 56

Die Drei-Säulen des Datenschutzes



Selbstregulierung und Selbstschutz vor allem im Internet

- Gesetze sind hier teilweise inhaltlich nicht passend / anwendbar (hinken der Realität hinterher)
- Problem der Gültigkeit der Gesetze (Gesetze sind länderspezifisch, Internet ist global)

21 / 56

Zulässigkeit der Datenverarbeitung

Grundsatz

Die Verarbeitung und Nutzung personenbezogener Daten ist prinzipiell verboten. (§4 Abs. 1 BDSG)

Ausnahmen:

- BDSG
- Andere Rechtsvorschrift
- Einwilligung der Betroffenen

→ Verbot mit Erlaubnisvorbehalt

22 / 56

Datenschutzgesetze

Bundesdatenschutzgesetz (BDSG)

- Öffentl. und nicht-öffentl. Bereich
- Privatwirtschaft
- Bundesverwaltung
- Vereine

Landesdatenschutzgesetze

- Nur öffentl. Bereich
- Landesverwaltung

23 / 56

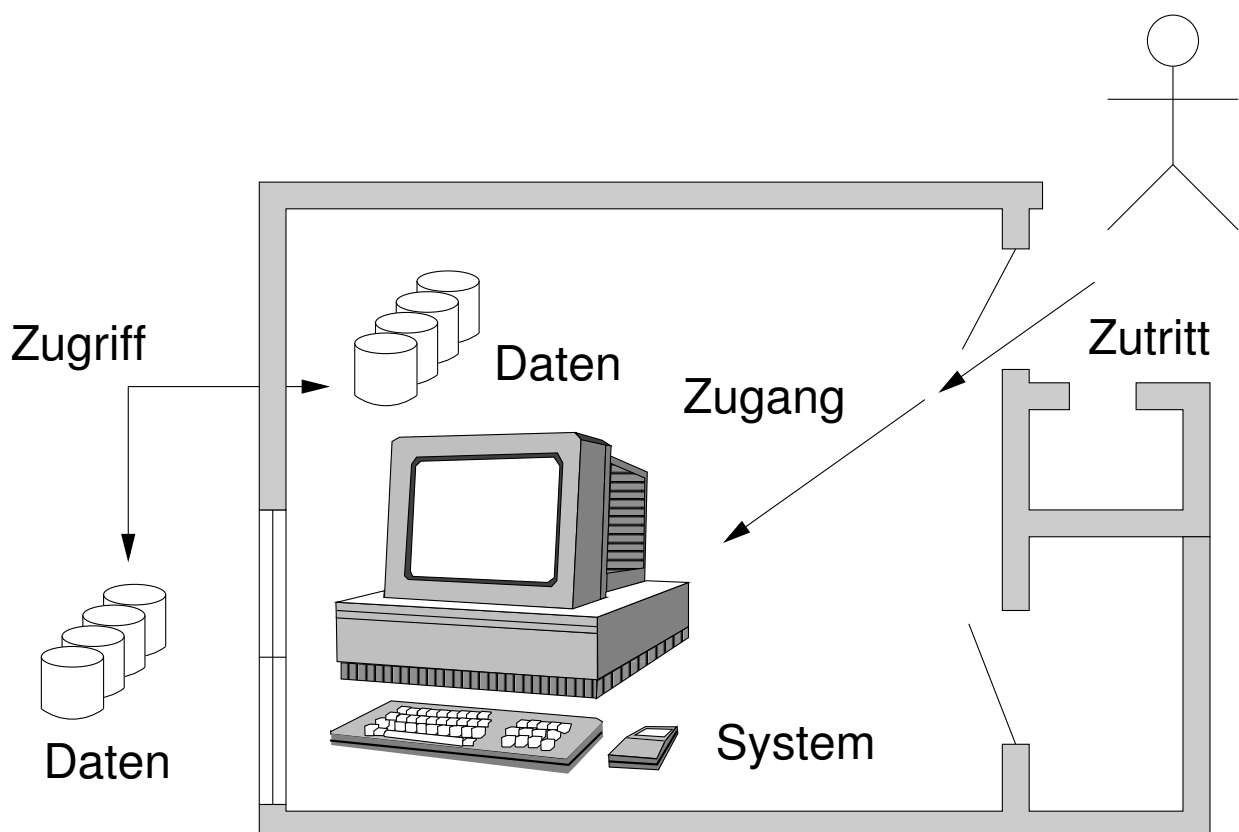
Technische und organisatorische Maßnahmen

Wenn die Erhebung zulässig ist, müssen für die Speicherung und Verarbeitung weitere Anforderungen erfüllt werden:

- Technische und organisatorischen Maßnahmen nach §9 BDSG
- Die 8 Gebote (Anhang zu §9 BDSG):
 - Zutrittskontrolle
 - Zugangskontrolle
 - Zugriffskontrolle
 - Weitergabekontrolle
 - Eingabekontrolle
 - Auftragskontrolle
 - Verfügbarkeitskontrolle
 - Trennungsgebot

24 / 56

Zutritt, Zugang, Zugriff



25 / 56

Erstes Gebot: Zutrittskontrolle

Du sollst keinen Unbefugten ins System vor Ort reinlassen.

- Sicherheitsschlösser mit Schlüsselregelung
- verschlossene Türen bei Abwesenheit
- Fenstersicherung (Erdgeschoss)
- Festlegung von Sicherheitsbereichen
- Zutrittsberechtigungsregelung
- Ausweisleser
- Protokollierung der Zu- und Abgänge
- Zutrittsregelungen für betriebsfremde Personen
- Empfang
- Codeschloss

26 / 56

Zweites Gebot: Zugangskontrolle

Du sollst keinen Unbefugten ans System ranlassen.

- Tastatursicherung durch Schloss
- Identifizierung und Authentifizierung
- Begrenzung der Fehlversuche
- Protokollierung
- Systemverwalterbefugnisse / -protokollierung
- Dunkelschaltung des Bildschirms mit Passwortschutz
- Firewall

27 / 56

Drittes Gebot: Zugriffskontrolle

Du sollst keinen Unbefugten auf deine Daten zugreifen lassen.

- Berechtigungskonzept
- Identifizierung und Authentifizierung
- Verschlüsselung
- Aufbewahrung in verschließbaren Schränken – „Data Safes“
- gesonderte Aufbewahrung der Sicherungsmedien

28 / 56

Weitergabekontrolle

Du sollst die Daten keinem Unbefugten weitergeben.

- Kennzeichnung der Datenträger
- Verschlüsselung von Daten auf Datenträgern
- Bestandsverzeichnis und Bestandskontrolle der Datenträger
- Festlegung der zur Abgabe von Datenträgern berechtigten Personen
- Festlegung des Empfängerkreises
- Regelungen für den Transport von Datenträgern
- Kryptographische Verschlüsselung der übertragenen Daten
- Fernwartungskonzept

29 / 56

Eingabekontrolle

Du sollst nachvollziehen können, wer auf Deine Daten zugreift.

- Identifizierung und Authentifizierung
- Protokollierung aller Eingaben / Veränderungen

30 / 56

Auftragskontrolle

Du sollst beauftragte Dritte kontrollieren.

- Schriftliche Festlegung der Weisungen / Vertrag
- Kontrolle der Einhaltung beim Auftragnehmer

31 / 56

Verfügbarkeitskontrolle

Dein System soll verfügbar sein.

- Betriebsbereitschaft
- Notfallkonzept
- Notfall-Rechenzentrum
- Unterbrechungsfreie Stromversorgung (USV)
- Brandmelder
- Datensicherung
- Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten

32 / 56

Trennungsgebot

Du sollst Daten, die verschiedenen Zwecken dienen, trennen.

Ziel: gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Gewährleistung der Zweckbindung)

Bei der Volkszählung 1987: strenges Abschottungsgebot

BDSG 2001: Physische oder logische Trennung

33 / 56

Betriebsverfassungsgesetz

Betriebsverfassungsgesetz

Grundlegende Ordnung der Zusammenarbeit von Arbeitgeber und Arbeitnehmern

35 / 56

Betriebsverfassungsgesetz (BetrVG)

§81 Unterrichts- und Erörterungspflicht des Arbeitgebers

Arbeitgeber muss Arbeitnehmer über dessen Aufgabe, Verantwortung und Art seiner Tätigkeit und ihre Einordnung in den Arbeitsablauf des Betriebs unterrichten.

36 / 56

Betriebsverfassungsgesetz (BetrVG)

§87 Mitbestimmungsrechte, insbes. §87 Abs. 1 Nr. 6

Betriebsrat hat mitzubestimmen bei

5. ...
6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;
7. ...

37 / 56

Betriebsverfassungsgesetz (BetrVG)

§89 Arbeitsschutz

Gegenstand: Maßnahmen

- zur Verhütung von Unfällen bei der Arbeit und
- arbeitsbedingten Gesundheitsgefahren zur menschengerechten Gestaltung der Arbeit.

Pflichten:

- Arbeitgeber muss Betriebsrat in Fragen des Arbeitsschutz und der Unfallverhütung hinzu ziehen
- Betriebsrat muss zum Arbeitsschutz und zur Unfallverhütung beitragen

38 / 56

Betriebsverfassungsgesetz (BetrVG)

§90 Unterrichts- und Beratungsrechte

- Arbeitgeber muss Betriebsrat über Planung von Arbeitsverfahren und Arbeitsabläufen rechtzeitig unterrichten;
- Arbeitgeber muss mit Betriebsrat vorgesehene Maßnahmen und ihre Auswirkungen auf die Arbeitnehmer so rechtzeitig beraten, dass Vorschläge und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können;
- Arbeitgeber und Betriebsrat sollen dabei gesicherte arbeitswissenschaftliche Erkenntnisse über menschengerechte Gestaltung der Arbeit berücksichtigen.

39 / 56

Betriebsverfassungsgesetz (BetrVG)

§91 Korrigierendes Mitbestimmungsrecht

Werden Arbeitnehmer durch Änderungen der Arbeitsplätze, des Arbeitsablaufs oder der Arbeitsumgebung, die den gesicherten arbeitswissenschaftlichen Erkenntnissen über menschengerechte Gestaltung der Arbeit offensichtlich widersprechen, in besonderer Weise belastet, so kann der Betriebsrat angemessene Maßnahmen zur Abwendung, Milderung oder zum Ausgleich der Belastung verlangen.

40 / 56

Betriebsverfassungsgesetz (BetrVG)

§98 Durchführung betrieblicher Bildungsmaßnahmen

Betriebsrat bestimmt bei der Durchführung von Maßnahmen der betrieblichen Berufsbildung mit.

41 / 56

Arbeitsschutzgesetz

- §5 Beurteilung der Arbeitsbedingungen: Arbeitgeber muss ermitteln, welche Schutzmaßnahmen notwendig sind
- §6 Dokumentation: Maßnahmen und ihre Überprüfung müssen dokumentiert werden
- §11 Arbeitsmedizinische Vorsorge: Arbeitgeber muss auf Wunsch arbeitsmedizinische Untersuchung veranlassen
- §12 Unterweisung: Arbeitgeber muss über Sicherheit und Gesundheitsschutz unterweisen

43 / 56

Bildschirmarbeitsverordnung

§2 Begriffsbestimmungen:

Was ist ein Bildschirm? Was ist ein Bildschirmarbeitsplatz?

- §3 Beurteilung der Arbeitsbedingungen:
Sicherheits- und Gesundheitsbedingungen insbesondere hinsichtlich einer möglichen Gefährdung des Sehvermögens sowie körperlicher Probleme und psychischer Belastungen sind zu ermitteln und zu beurteilen.
- §4 Anforderungen an die Gestaltung (Anhang)
- §5 Täglicher Arbeitsablauf:
Bildschirmarbeit ist durch andere Tätigkeiten oder Pausen zu unterbrechen
- §6 Untersuchung der Augen und des Sehvermögens vor Antritt, danach regelmäßig, bei Auftritt von Sehbeschwerden

46 / 56

§2 Begriffsbestimmungen

1. Bildschirmgeräte im Sinne dieser Verordnung ist ein Bildschirm zur Darstellung alphanumerischer Zeichen oder zur Grafikdarstellung, ungeachtet des Darstellungsverfahrens.

Der Begriff "Bildschirmgeräte" umfaßt alle Bildschirme- egal, welches technische Darstellungsverfahren gewählt wurde (Kathodenstrahlröhre, Flüssigkeitsanzeige etc.) Er schließt auch solche mit ein, die nicht nur im Büro, sondern auch zur Prozeßsteuerung und in nicht elektronischen Darstellungssystemen wie z.B. Microfilmlesegeräte eingesetzt werden.

2. Bildschirmarbeitsplatz im Sinne dieser Verordnung ist ein Arbeitsplatz mit einem Bildschirmgerät, der ausgestattet sein kann mit

- a. Einrichtung zur Erfassung von Daten,
- b. Software, die den Beschäftigten bei der Ausführung ihrer Arbeitsaufgaben zur Verfügung steht,
- c. Zusatzgeräten und Elementen, die zu Betreiben oder Benutzen des Bildschirmgeräts gehören, oder
- d. Sonstigen Arbeitsmitteln,
- e. sowie die unmittelbare Arbeitsumgebung.

Neben den schon genannten Komponenten gehört auch die unmittelbare Arbeitsumgebung mit ihrem möglichen Einfluß auf die Arbeit am Bildschirm dazu. Weitere Komponenten sind Tastatur, Maus, Lichtgriffel, Belegleser, Scanner etc. Bei der Software die das Zusammenwirken zwischen Mensch und Maschine erst ermöglicht, handelt es sich um Anwenderprogramme und Betriebssysteme. Zusatzgeräte und Elemente sind Drucker, Plotter, externe Speichergeräte. Zu den sonstigen Arbeitsmitteln gehören Arbeitstisch, Arbeitsstuhl, Fußstütze etc. .

3. Beschäftigte im Sinne dieser Verordnung sind Beschäftigte, die gewöhnlich bei einem nicht unwesentlichen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.

DIN EN ISO 9241

Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten

Teil	Titel	DIN EN ISO
1	Allgemeine Einführung	2/02
2	Anforderungen an die Arbeitsaufgaben - Leitsätze	6/93
3	Anforderungen an visuelle Anzeigen	8/93
4	Anforderungen an die Tastatur	1/99
5	Anforderungen an Arbeitsplatzgestaltung und Körperhaltung	8/99
6	Leitsätze für die Arbeitsumgebung	3/01
7	Anforderungen an visuelle Anzeigen bez. Reflexionen	12/98
8	Anforderungen an Farbdarstellungen	4/98
9	Anforderungen an Eingabemittel, ausgen. Tastaturen	3/02

48 / 56

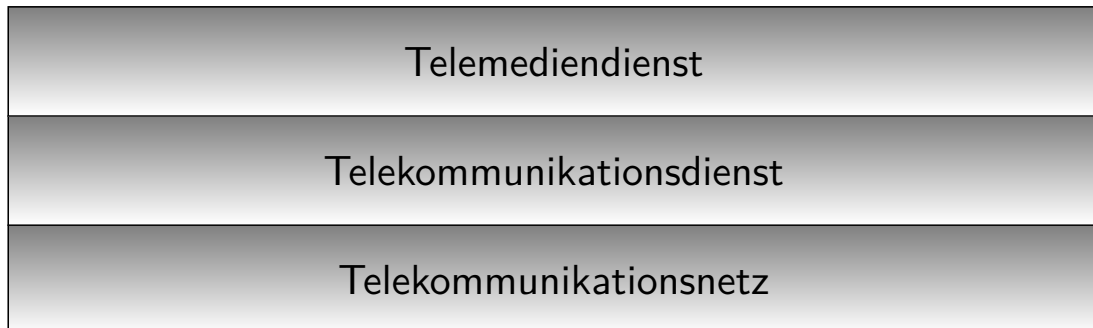
DIN EN ISO 9241

Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten

Teil	Titel	DIN EN ISO
10	Grundsätze der Dialoggestaltung	7/96
11	Anforderungen an die Gebrauchstauglichkeit - Leitsätze	1/99
12	Informationsdarstellung	8/00
13	Benutzerführung	8/00
14	Dialogführung mittels Menüs	12/00
15	Dialogführung mittels Kommandosprachen	8/99
16	Dialogführung mittels direkter Manipulation	3/00
17	Dialogführung mittels Bildschirmformularen	4/00

49 / 56

Telekommunikationsdienst oder Telemediendienst



52 / 56

Telekommunikation

Telekommunikation

Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen.

Telekommunikationsgesetz betrifft

- technischen Vorgang der Übertragung
- Telekommunikations-Dienstleistungen, d.h. das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte (Access-Provider und Netzbetreiber)
- nicht: Aufbereitung oder Verwendung von übertragenen Inhalten

53 / 56

Telemedien

Telemedien

Telemedien ist ein Rechtsbegriff für elektronische Informations- und Kommunikationsdienste.

Ehemals Teledienste

- elektronische Post
- Telebanking
- Telearbeit
- Telemedizin
- Fernlernen
- Telespiele
- Angebote von Waren und Dienstleistungen

Ehemals Mediendienste

- Zeitungen / Zeitschriften
- redaktionell bearbeitete Newsletter, z.B. Angebote von Reiseunternehmen mit Informationen zur Geschichte und Politik eines Landes
- Pressemitteilungen online
- private Websites
- Blogs

54 / 56

Früher wurden in den Gesetzen Teledienste und Mediendienste unterschieden. Teledienste waren alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Unter Mediendienste verstand man alle elektronischen Verteildienste und solche, bei denen die redaktionelle Gestaltung zur Meinungsbildung im Vordergrund steht. Sie richten sich an die Allgemeinheit, während Teledienste individualisiert sind. Für beide Arten von Diensten gab es unterschiedliche gesetzliche Regelungen. Da die Grenzen aber fließend sind, löste das Telemediengesetz (TMG) die bisherigen getrennten Regelungen ab. Das TMG regelt die rechtlichen Rahmenbedingungen für sogenannte Telemedien in Deutschland.

Zitat von <http://de.wikipedia.org/wiki/Mediendienst>:

Teledienstgesetz und Staatsvertrag über Mediendienste traten zum 1. März 2007 außer Kraft. Die Begriffe Teledienst und Mediendienst sind seitdem im umfassenden Begriff Telemedien des Telemediengesetzes aufgegangen. Die früheren Abgrenzungskriterien zwischen Telediensten, Mediendiensten und Rundfunk werden in der Fachliteratur teilweise noch zur Bestimmung derjenigen Telemedien herangezogen, für die besondere Anforderungen im Abschnitt Telemedien des Staatsvertrages über Rundfunk und Telemedien (§§54 – 61 RStV) zu beachten sind. Zu diesen Anforderungen gehören z.B. Informationspflichten nach §55 Rundfunkstaatsvertrag (RStV) (bei redaktionellen Angeboten muss zusätzlich ein für den Inhalt Verantwortlicher mit Name und Anschrift benannt werden) und die Verpflichtung zur Aufnahme einer Gegendarstellung nach §56 RStV.

Telemediengesetz (TMG)

Das TMG enthält unter anderem Vorschriften

- zum Impressum für Telemediendienste
- zur Bekämpfung von Spam (Verbot einer Verschleierung und Verheimlichung von Absender und Inhalt bei Werbe-E-Mails)
- zur Haftung von Dienstbetreibern für gesetzwidrige Inhalte in Telemediendiensten
- zum Datenschutz beim Betrieb von Telemediendiensten und zur Herausgabe von Daten
- zum Providerprivileg (Überbringer einer Nachricht ist nicht notwendigerweise haftbar für den Inhalt der Nachricht)

<http://www.gesetze-im-internet.de/tmg/index.html>

55 / 56

Zitat <http://de.wikipedia.org/wiki/Providerprivileg>:

Das Providerprivileg ist ein Begriff aus dem Online-Recht, bezeichnet aber eigentlich ein etwas grundlegendere Konzept, nämlich dass der Überbringer (Bote, Provider) inhaltlich nicht für das Überbrachte (die Nachricht) einstehen muss, die er übermittelt, aber nicht selbst erstellt.

1 Münch 2010 MÜNCH, Peter: Technisch-organisatorischer
Datenschutz: - Leitfaden für Praktiker. 4. Auflage. Datakontext,
2010. – ISBN 978-3895775864