Einführung in den Datenschutz (Zusatzveranstaltung zum Sopra)

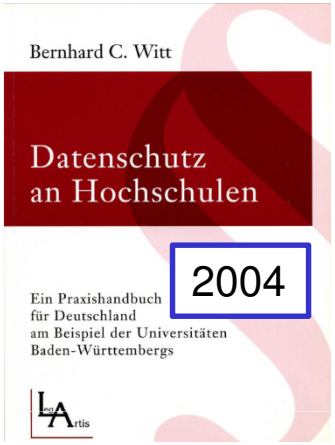
Vortrag im Wintersemester 2011/2012

an der Universität Ulm

von Bernhard C. Witt

Zum Vortragenden

it.sec
security for your information



Bernhard C. Witt

- Senior Consultant für Datenschutz und Informationssicherheit
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- Industriekaufmann, Diplom-Informatiker
- seit 1998 selbstständig, u.a. Autor diverser Fachbücher
- seit 2005 Lehrbeauftragter an der Universität Ulm (jedes Sommersemester: „Grundlagen des Datenschutzes und der IT-Sicherheit“, 6 LP)
- seit 2009 Sprecher der GI-FG Management von Informationssicherheit

Informationelles Selbstbestimmungsrecht (1)

Informationelles Selbstbestimmungsrecht

Grundrecht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen

Art. 2 Abs. 1 GG

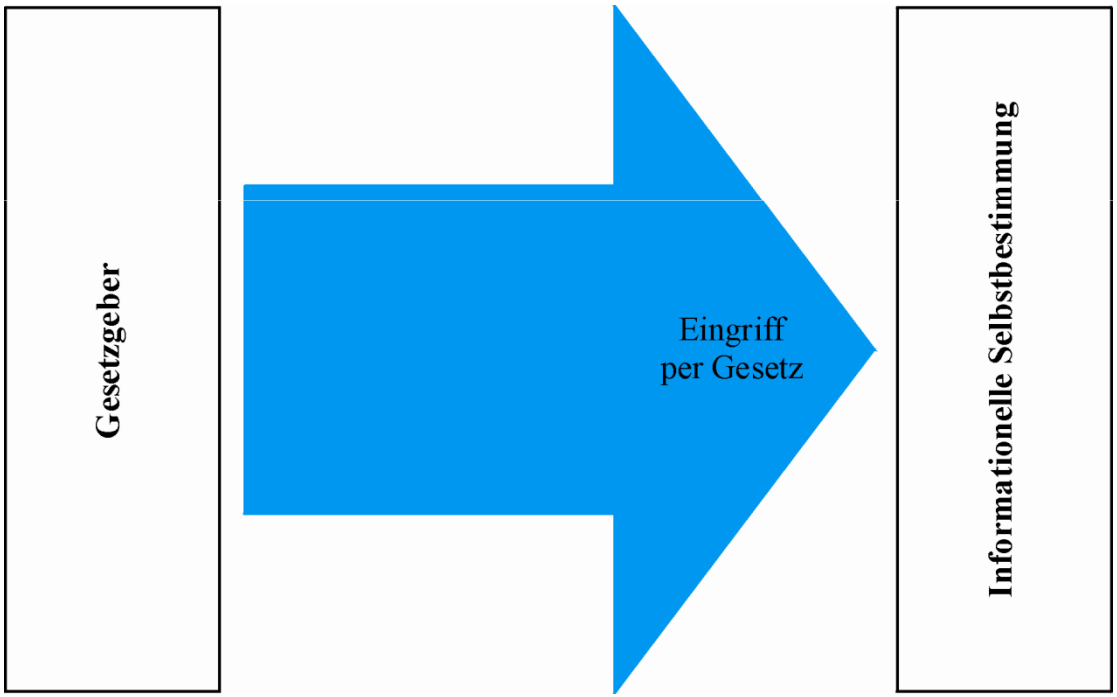
Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

i.V.m.

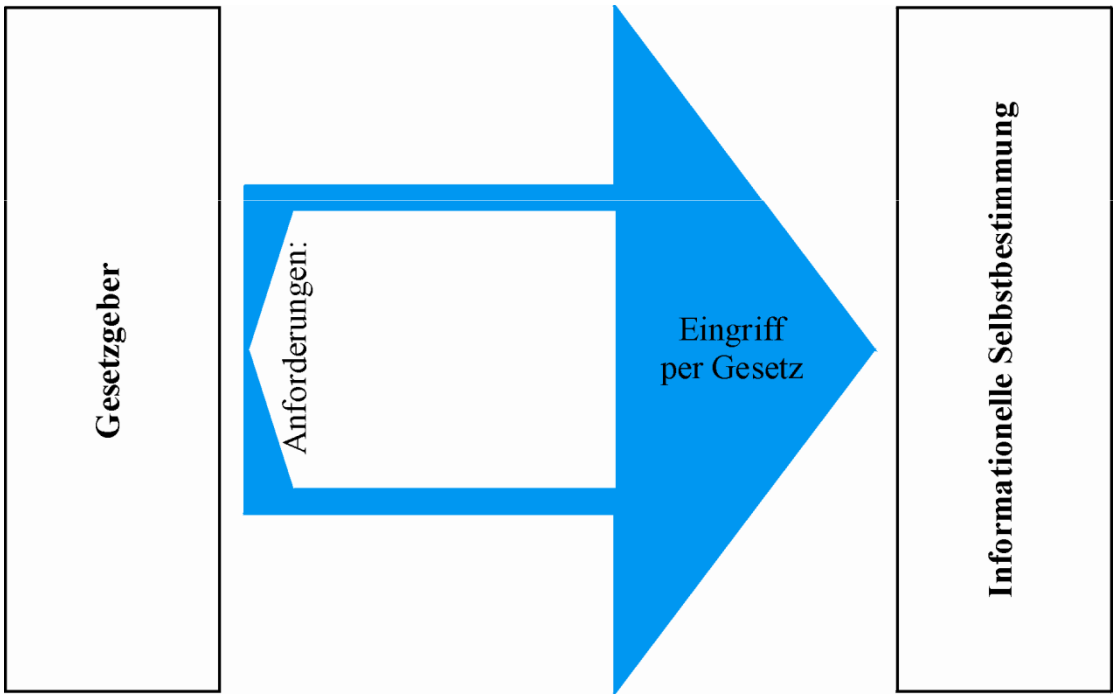
Art. 1 Abs. 1 GG

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Informationelles Selbstbestimmungsrecht (2)

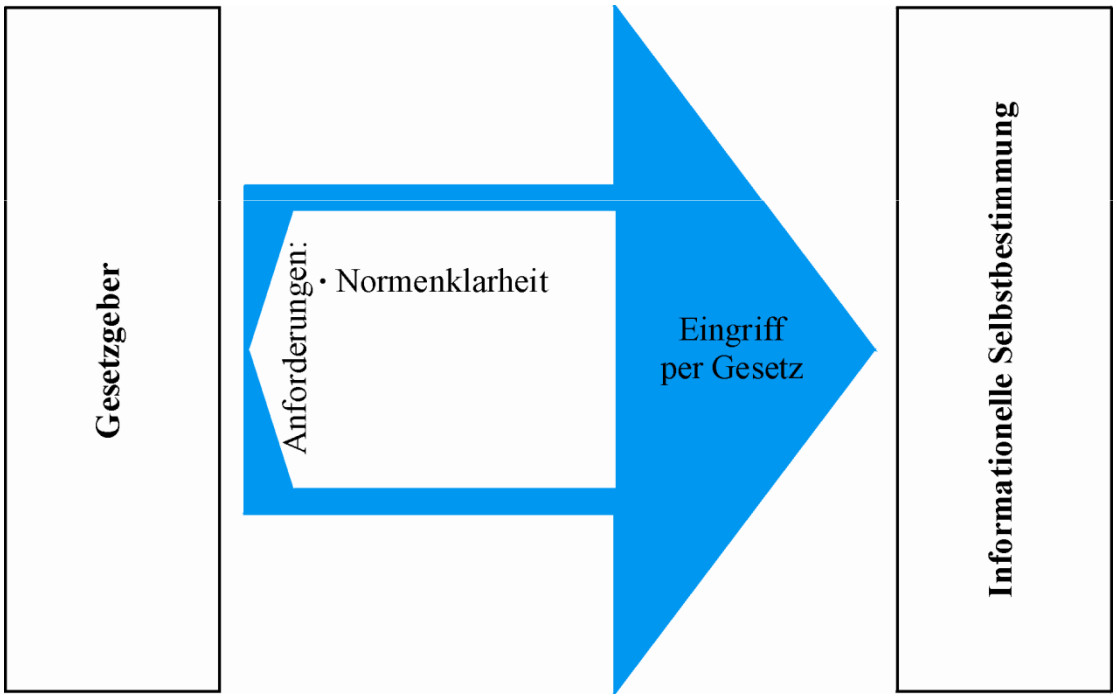


Informationelles Selbstbestimmungsrecht (3)



Eingriff erfordert:

Informationelles Selbstbestimmungsrecht (4)

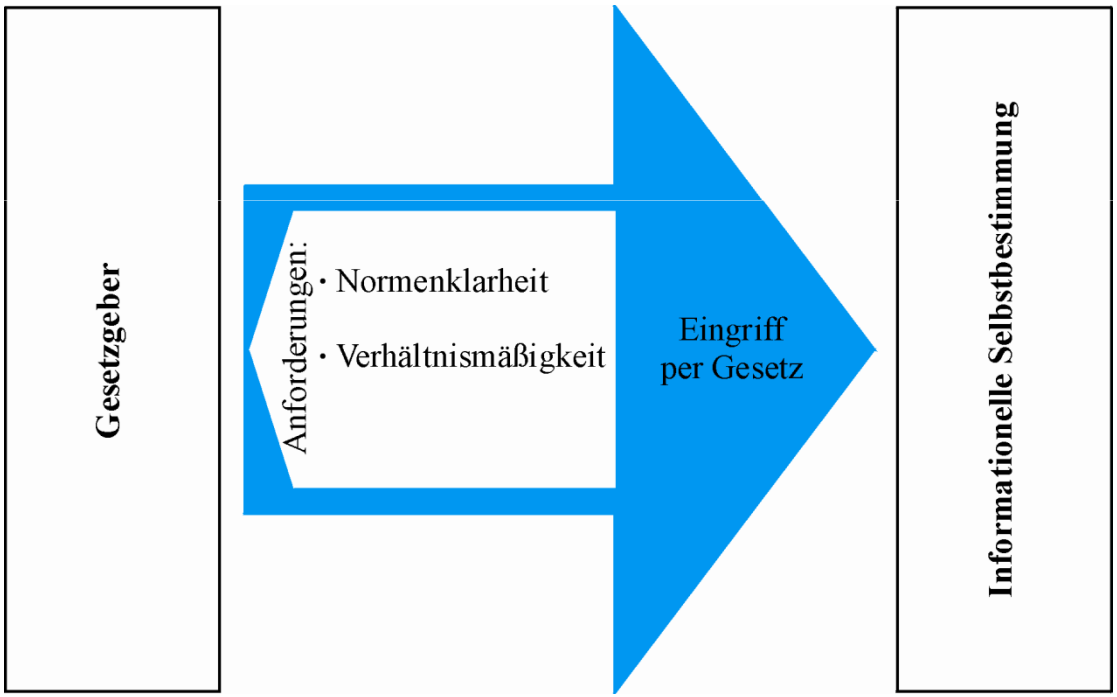


Eingriff erfordert:

Normenklar-heit

Verwendungs-zweck bereichs-spezifisch und präzise bestimmt

Informationelles Selbstbestimmungsrecht (5)

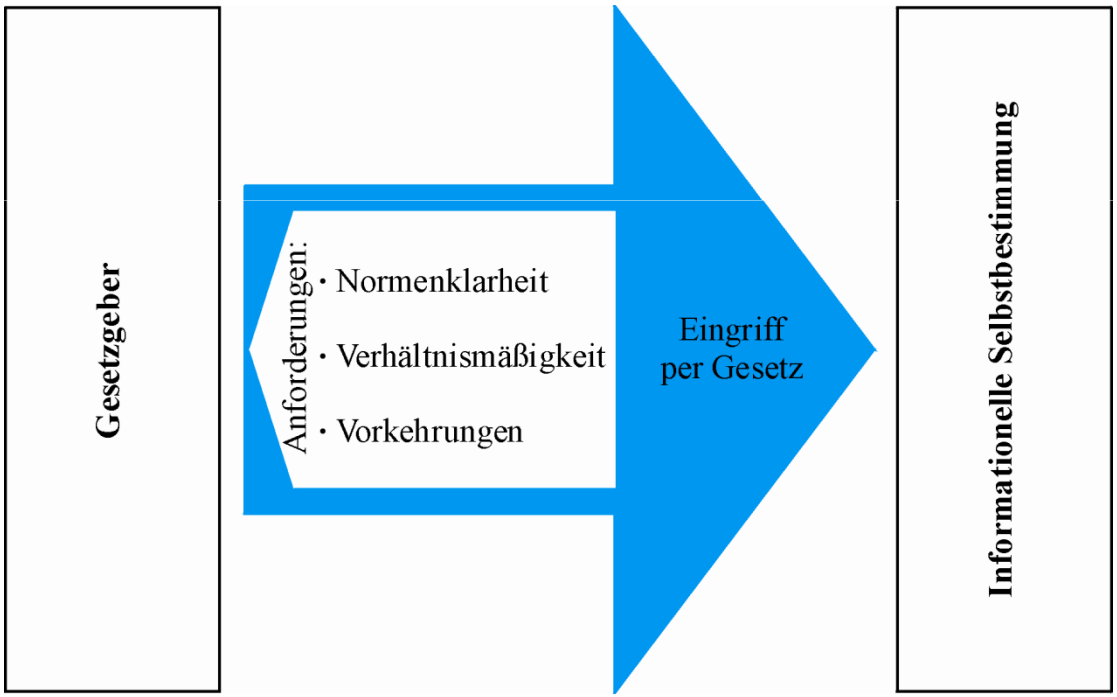


Eingriff erfordert:

Verhältnis-mäßigkeit

personenbezogene Daten müssen für Zweck geeignet und erforderlich sein

Informationelles Selbstbestimmungsrecht (6)

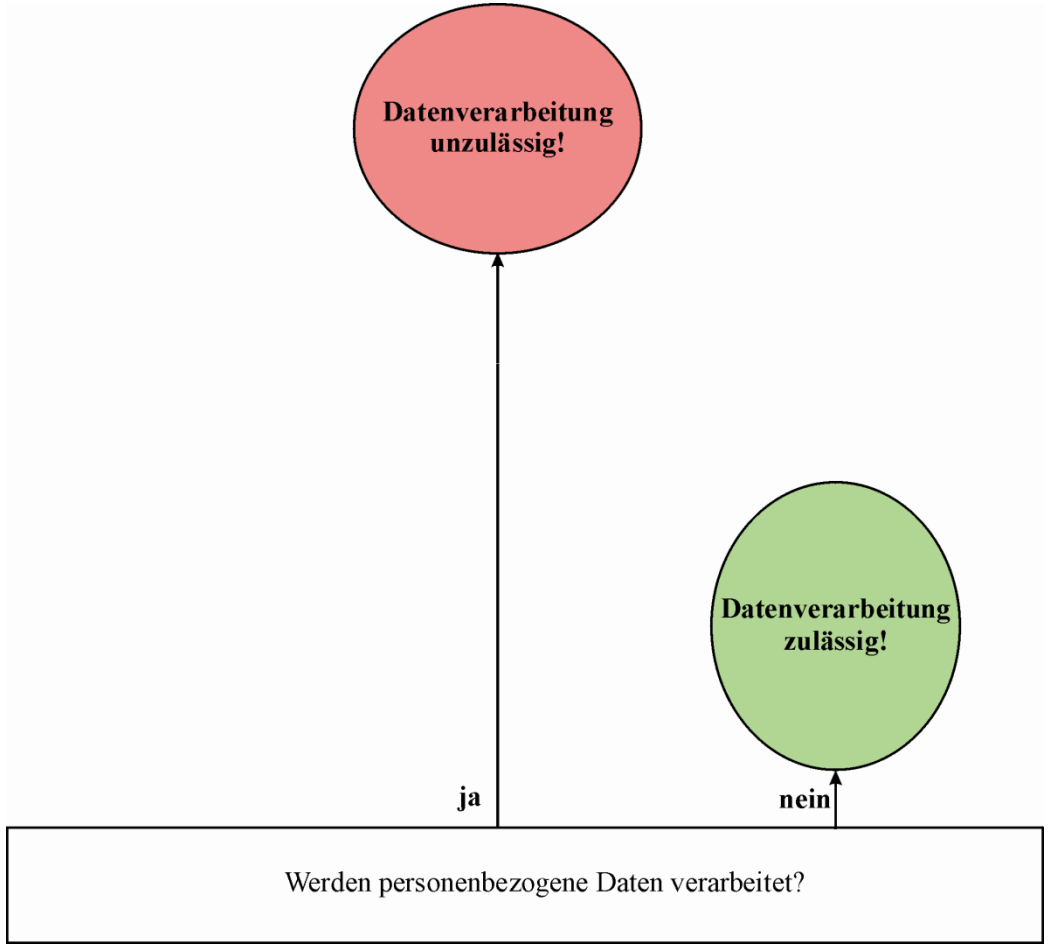


Eingriff erfordert:

Vorkehrungen

organisatorische & verfahrensabhängige Maßnahmen, insbesondere im Sinne der Datensparsamkeit

Verbot mit Erlaubnisvorbehalt (1)

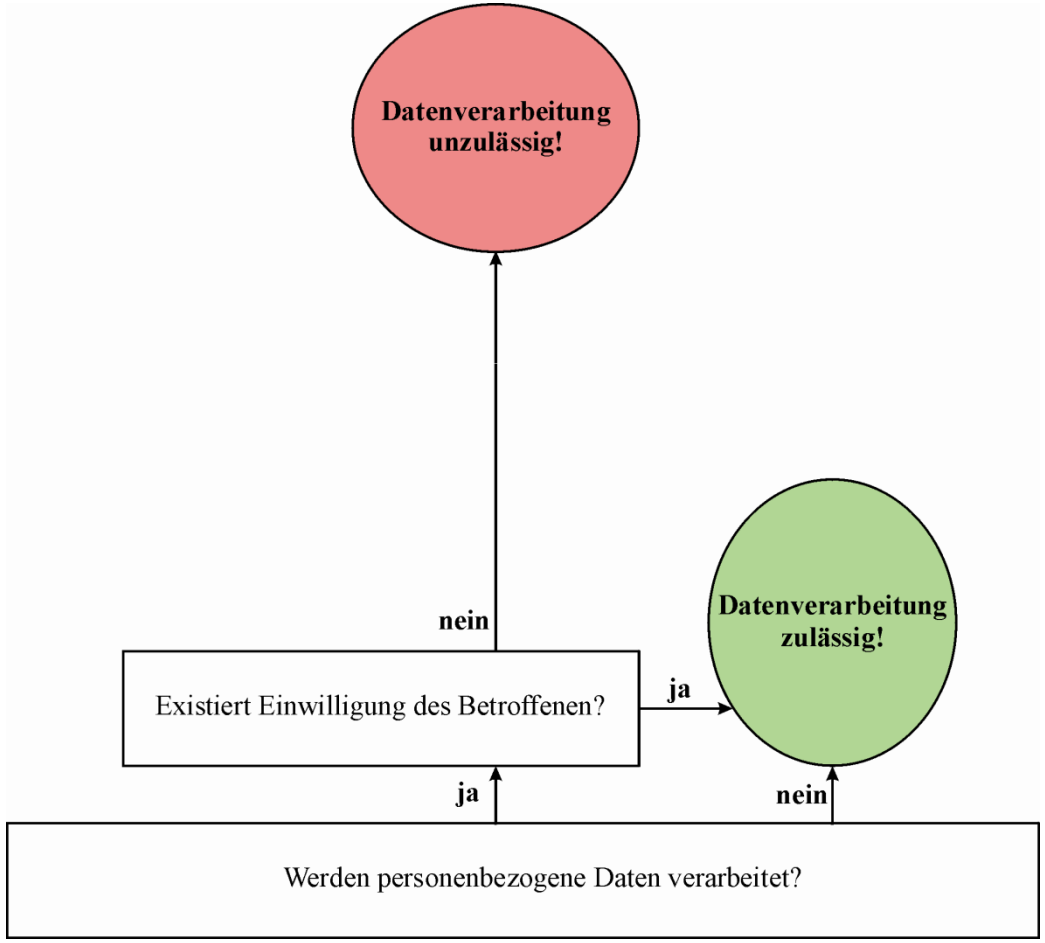


Grundsatz:

Die Verarbeitung personenbezogener Daten ist grundsätzlich **verboten**!

Eine Gestattung ist jedoch unter Umständen möglich.

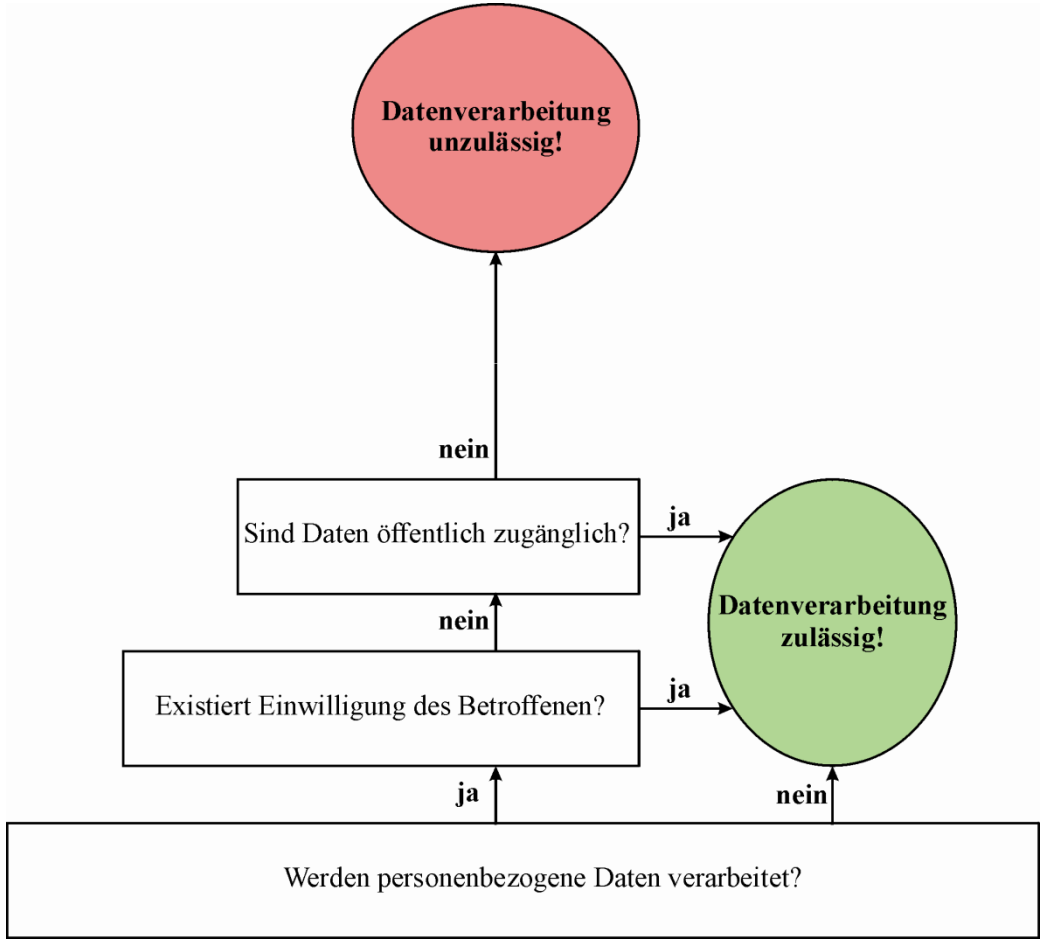
Verbot mit Erlaubnisvorbehalt (2)



Anforderungen an die Einwilligung:

- der Betroffene muss frei entscheiden können
- dem Betroffenen muss vorher der Zweck der geplanten Verarbeitung mitgeteilt werden
- der Betroffene soll über seine Rechte sowie die Folgen einer Ablehnung aufgeklärt werden
- die Einwilligung soll schriftlich erfolgen

Verbot mit Erlaubnisvorbehalt (3)



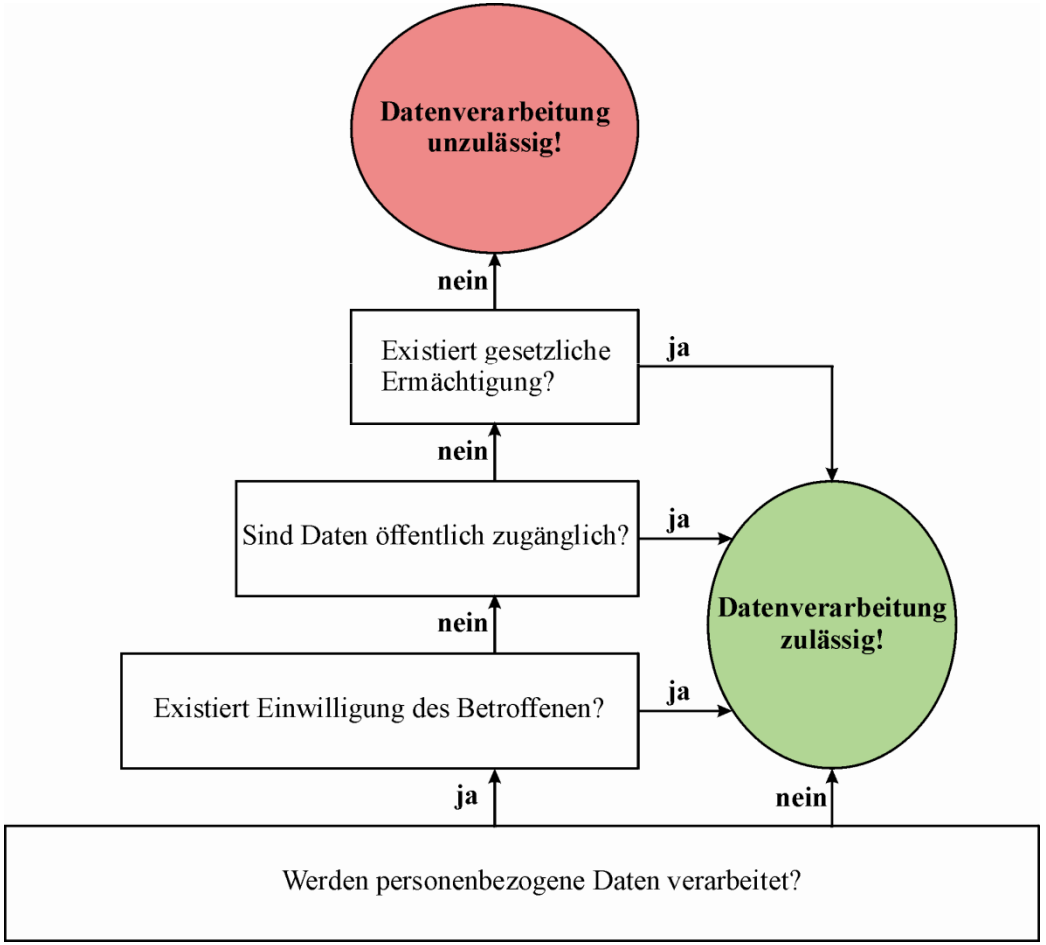
Öffentliche Quellen:

- Adress- und Telefonbücher
- öffentliche Register
- Veröffentlichungen
- Internet (sofern nicht passwortgeschützt)

Hinweis:

- bei besonderen Arten personenbezogener Daten (z.B. Religionszugehörigkeit, Gesundheitsdaten) sind Daten nur öffentlich, wenn sie durch den Betroffenen selbst öffentlich gemacht wurden
- Unzulässig veröffentlichte Daten bleiben unzulässig
- Für Werbungszwecke sind öffentliche Quellen auf Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse beschränkt

Verbot mit Erlaubnisvorbehalt (4)



Gesetzliche Erlaubnis:

- entweder im Datenschutzgesetz selbst
- oder in einer anderen Rechtsvorschrift (Gesetz, Verordnung, Satzung eines autonomen öffentlich-rechtlichen Verbandes mit gesetzlicher Ermächtigung*), die verfassungsgemäß (also normenklar & verhältnismäßig) ist

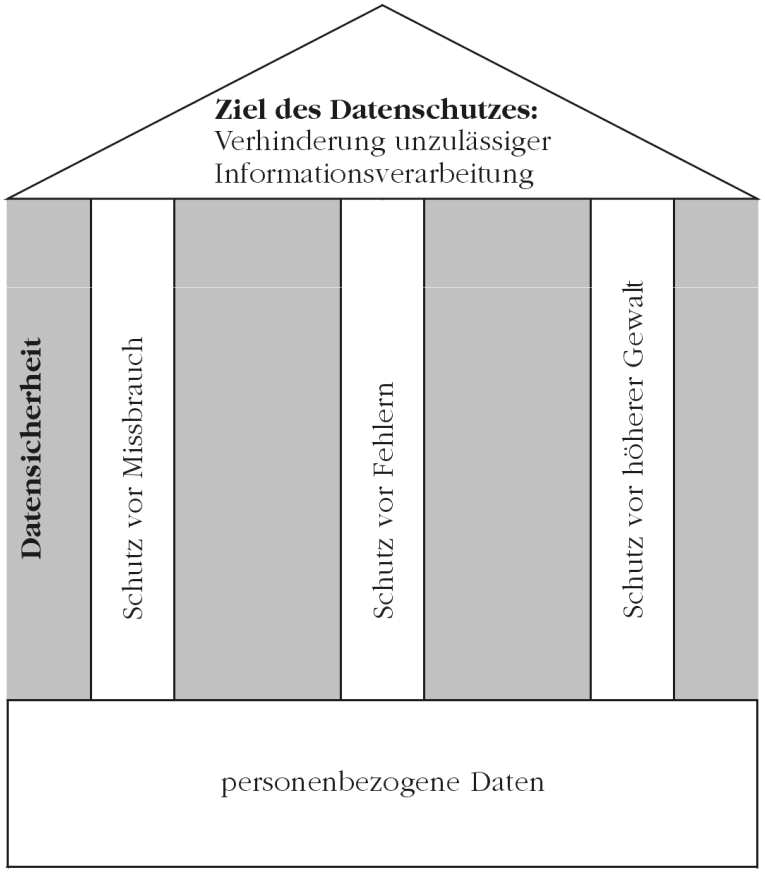
→ stellt **Regelfall** dar!

* Uni verfügt über ein solches Satzungsrecht (§ 8 V LHG)

Zweckbindung

- Erfordernis zur **Zweckfestlegung** bei der Erhebung
- Zweck abhängig von geplanter **Verwendung**
- **Verfahren** *(= festgelegte Art & Weise, wie Tätigkeit / Prozess auszuführen ist)*
  im Datenschutzrecht kontextsensitiv
  → zweckbezogen verknüpfte Verarbeitungsschritte
  → Umgang mit Datum von Erhebung bis Löschung
  (kompletter Life Cycle eines Datums)
- Jeder Verarbeitungsschritt unterliegt **Zweckbindung**
- **Zweckänderung** bei öffentlichen Stellen nur in Ausnahmefällen zulässig

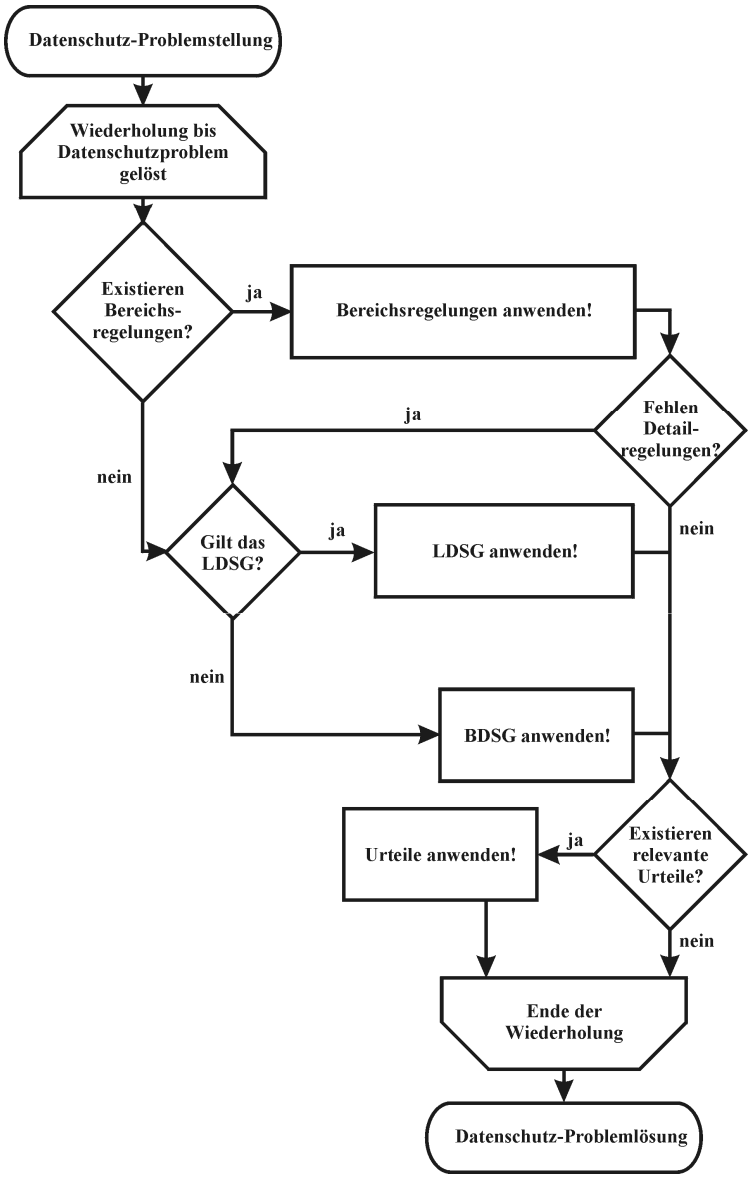
Zusammenhang zwischen Datensicherheit und Datenschutz



Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung** unrichtiger personenbezogener Daten, auf **Löschung** unzulässiger personenbezogener Daten oder auf **Sperrung** nicht mehr benötigter personbezogener Daten
- Recht auf **Anrufung** des zuständigen Datenschutzbeauftragten
- Recht auf **Schadensersatz** bei schweren Verstößen

Niemand darf wegen der Geltendmachung seiner Rechte benachteiligt werden!



Anzuwendendes Datenschutzrecht

Fallbezogen für Hiwi-Börse:
Uni = Landesbehörde → **LDSG**!
Zulässigkeit → § 4 LDSG
Erhebung → §§ 13 & 14 LDSG
Verwendung → § 15 LDSG
Betroffene → §§ 5 & 21ff LDSG
Schutzmaßnahmen → § 9 LDSG
Hiwi = Arbeitnehmer → § 36 LDSG
+ § 86 LBG
Uni-Mitglieder/-Angehörige → **LHG**!
stud. / wiss. Hiwis → § 57 LHG
Uni-Datenverarbeitung → § 12 LHG
+ **Hochschul-Datenschutzverordnung**
Online-Börse = Webportal → **TMG**!
Nutzung Webportal → § 13 TMG
Zugang Webportal → § 14 TMG

Anforderungen des LDSG (1)

- **§ 4 Abs. 1 LDSG**: Die Verarbeitung personenbezogener Daten ist nur zulässig,
  1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
  2. soweit der Betroffene eingewilligt hat
- **§ 13 Abs. 1 LDSG**: Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist
- **§ 13 Abs. 2 LDSG**: Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind beim Betroffenen mit seiner Kenntnis zu erheben
- **§ 14 Abs. 1 Nr. 1 LDSG**: Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, sind ihm gegenüber anzugeben:
  1. die beabsichtigte Datenverarbeitung und der Zweck der Verarbeitung
- **§ 15 Abs. 2 Nr. 2 LDSG**: Das Speichern, Verändern und Nutzen personenbezogener Daten für andere Zwecke ist nur zulässig, wenn
  2. der Betroffene eingewilligt hat oder offensichtlich ist, dass dies im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er seine Einwilligung hierzu verweigern würde

Anforderungen des LDSG (2)

- **§ 5 Abs. 1 LDSG**: Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf
  1. Auskunft über die zu seiner Person gespeicherten Daten (§ 21),
  2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§§ 22 bis 24),
  3. Auskunft aus dem Verfahrensverzeichnis (§ 11 Abs. 4),
  4. Einwendung eines schutzwürdigen, in seiner persönlichen Situation begründeten Interesses gegenüber der Verarbeitung seiner Daten (§ 4 Abs. 6),
  5. Schadensersatz (§ 25),
  6. Anrufung des Landesbeauftragten für den Datenschutz (§ 27)
- **§ 9 Abs. 1 LDSG**: Die Gestaltung und Auswahl der technischen Einrichtungen und der Verfahren zur automatisierten Verarbeitung personenbezogener Daten hat sich an dem Grundsatz auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten
- **§ 9 Abs. 2 LDSG**: Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Erforderlich sind Maßnahmen, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anforderungen des LDSG (3)

- **§ 9 Abs. 3 LDSG**: Werden personenbezogene Daten automatisiert verarbeitet, sind je nach Art und Verwendung der zu schützenden personenbezogenen Daten und unter Berücksichtigung des Standes der Technik Maßnahmen zu treffen, die geeignet sind,
  1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren (**Zutrittskontrolle**),
  2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Datenträgerkontrolle**),
  3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (**Speicherkontrolle**),
  4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (**Benutzerkontrolle**),
  5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (**Zugriffskontrolle**),
  6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (**Übermittlungskontrolle**),
  7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (**Eingabekontrolle**),
  8. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
  9. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**),
  10. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**), und
  11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (**Organisationskontrolle**).

Anforderungen des LDSG (4)

- **§ 36 Abs. 1 LDSG**: Personenbezogene Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung es vorsieht
- **§ 36 Abs. 2 LDSG**: Auf die Verarbeitung von Personalaktendaten von Angestellten und Arbeitern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.
  Hinweis:
  § 86 Abs. 2 LBG: Personalaktendaten sind zu löschen, wenn sie für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind, spätestens jedoch nach Ablauf einer Aufbewahrungsfrist von fünf Jahren.
  § 86 Abs. 8 LBG: Personalaktendaten dürfen nach ihrer Löschung bei Personalmaßnahmen nicht mehr berücksichtigt werden (Verwertungsverbot).

Anforderungen des LHG (1)

- **§ 57 LHG**: Personen mit einem ersten Hochschulabschluss können als wissenschaftliche Hilfskraft eingestellt werden. Als studentische Hilfskraft kann eingestellt werden, wer in einem Studiengang immatrikuliert ist, der zu einem ersten Hochschulabschluss führt; das Arbeitsverhältnis endet spätestens mit der Exmatrikulation. Die Beschäftigung ist bis zur Dauer von sechs Jahren zulässig und erfolgt in befristeten Angestelltenverhältnissen mit weniger als der Hälfte der regelmäßigen Arbeitszeit der Angestellten im öffentlichen Dienst. Wissenschaftliche sowie studentische Hilfskräfte üben Hilfstätigkeiten für Forschung und Lehre aus und unterstützen Studierende in Tutorien. Wissenschaftlichen Hilfskräften, die ihre Hilfstätigkeiten überwiegend im Bereich der Lehre erfüllen, kann der Fakultätsvorstand die Bezeichnung „Lehrassistent“ oder „Lehrassistentin“ verleihen.

Anforderungen des LHG (2)

- **§ 12 Abs. 1 LHG**: Studienbewerber, Studierende, Prüfungskandidaten, Mitglieder und Angehörige der Hochschule und der Hochschulverwaltung und externe Nutzer von Hochschuleinrichtungen sowie die staatlichen und kirchlichen Prüfungsämter sind verpflichtet, der Hochschule die zur Erfüllung ihrer Aufgaben erforderlichen personenbezogenen Daten, insbesondere zum Hochschulzugang, zum Studium, zum Studienverlauf, zu den Prüfungen und zur Nutzung weiterer Angebote der Hochschule anzugeben. […] Das Wissenschaftsministerium bestimmt durch Rechtsverordnung die nach Satz 1 anzugebenden Daten und die Zwecke ihrer Verarbeitung […]
  Hinweis:
  Die spezifischen Vorschriften zur Verarbeitung von Studierendendaten können der zugehörigen **Hochschul-Datenschutzverordnung** entnommen werden!
- **§ 12 Abs. 2 LHG**: Die Nutzung der nach Absatz 1 erhobenen Daten für andere Zwecke und die Übermittlung an eine andere Hochschule ist auch zulässig, wenn und soweit die Daten von der Hochschule oder der anderen Hochschule auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht bei den Betroffenen erhoben werden dürfen. Im Übrigen gilt das Landesdatenschutzgesetz.

Anforderungen der Hochschul-Datenschutzverordnung

- **§ 12 Abs. 1 Hochschul-Datenschutzverordnung**: Die Hochschule darf folgende Daten von Studierenden 40 Jahre – vom Zeitpunkt der Exmatrikulation ab gerechnet – verarbeiten:
  1. Familienname, Vorname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht,
  2. Studiengang, Matrikelnummer,
  3. Praxissemester, Urlaubssemester oder sonstige Studienunterbrechungen,
  4. Ergebnis und Datum der Diplom-Vorprüfung oder Zwischenprüfung,
  5. Ergebnis und Datum der Abschlussprüfung mit Gesamtnote und den die Gesamtnote tragenden Einzelnoten,
  6. Datum der Immatrikulation und Exmatrikulation sowie Exmatrikulationsgrund.

  Diese Daten sind nach der Exmatrikulation gemäß § 20 Abs. 3 des Landesdatenschutzgesetzes unverzüglich zu sperren, es sei denn, das Prüfungsverfahren ist noch nicht abgeschlossen; in diesem Falle sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren. Alle sonstigen Daten sind nach der Exmatrikulation unverzüglich zu löschen, es sei denn, das Prüfungsverfahren ist noch nicht abgeschlossen; in diesem Falle sind die Daten nach Abschluss des Prüfungsverfahrens unverzüglich zu löschen.

Anforderungen des TMG (1)

- **§ 13 Abs. 1 TMG**: Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten … in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.
- **§ 13 Abs. 2 TMG**: Die Einwilligung kann elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass
  1. der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
  2. die Einwilligung protokolliert wird,
  3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
  4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann
- **§ 13 Abs. 3 TMG**: Der Diensteanbieter hat den Nutzer vor Erklärung der Einwilligung auf das Recht nach Absatz 2 Nr. 4 hinzuweisen. Absatz 1 Satz 3 gilt entsprechend.

Anforderungen des TMG (2)

- **§ 13 Abs. 4 TMG**: Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass
  1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
  2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
  3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
  4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
  5. Daten nach § 15 Abs. 2 nur für Abrechnungszwecke zusammengeführt werden können und
  6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

  An die Stelle der Löschung nach Satz 1 Nr. 2 tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.
- **§ 14 Abs. 1 TMG**: Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten)