Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

Europäische Datenschutzgrundverordnung und Smartness

Dr. Imke Sommer

17. Datenschutzkongress

Berlin, 27. April 2016

Zwei Begriffe, die es in sich haben

- Europäische Datenschutzgrundverordnung
- Smartness

Europäische Datenschutz-grundverordnung

http://fs.cs.uni-frankfurt.de/artikel/don%C2%B4t-panic

Die Europäische Grundrechtecharta

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

Internetvertrauensbildende Maßnahme:

Die Europäische Grundrechtecharta

Titelbild des 38. Jahresberichtes der bremischen LfDI, Gestaltung: Marco Seifert

Datenschutz ist Grundrechtsschutz- auch in Europa (1)

Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (= “IT- Grundrecht”)

Europäische Grundrechtecharta:

Rechte auf Schutz personenbezogener Daten und

auf Achtung des Privatlebens und der Kommunikation

Cartoon von Fernandez, Lappan Verlag GmbH, Oldenburg

Datenschutz ist Grundrechtsschutz – auch in Europa (2)

*„Darauf verzichtet, etwas im Netz erneut nachzuschlagen, aus Angst, die Google-Mitarbeiter könnten mich für doof halten.“**

Grundrecht auf informationelle Selbstbestimmung

= „das Recht, selbst zu bestimmen, wer wann was über mich weiß“

Europäische Grundrechtecharta:

Rechte auf Schutz personenbezogener Daten und

auf Achtung des Privat-lebens und der Kommunikation

*Zitat / Tweet von Benjamin Nickel

Informationelle Selbstbestimmung

- Recht auf Achtung der Kommunikation = Kommunikationsgrundrecht = Äußerungsgrundrecht
- Selbstbestimmung <–> Fremdbestimmung

ZEIT ONLINE: Sie sagen, Big Data sei eine Revolution. Warum?

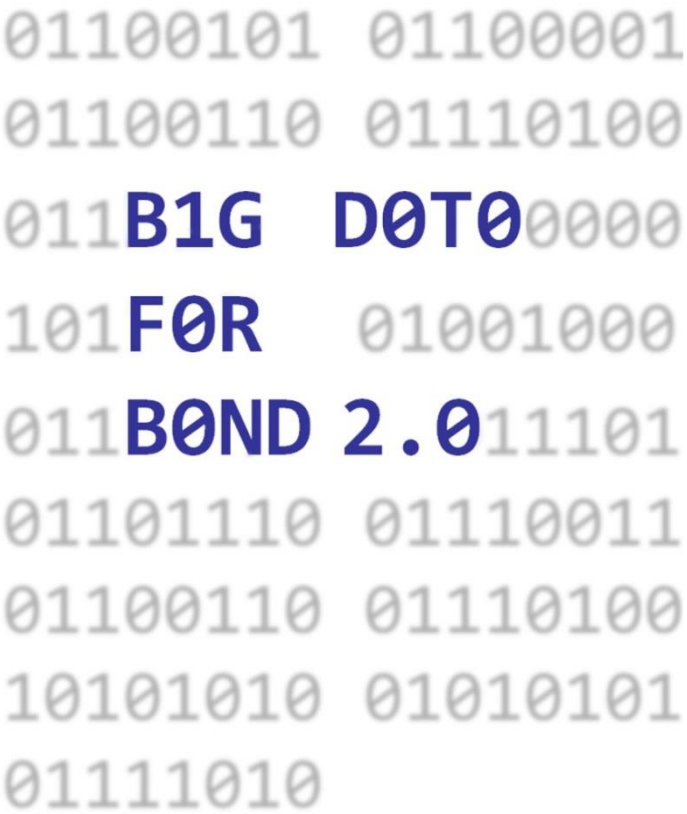
Viktor Mayer-Schönberger: Weil es verändert, wie wir Wirklichkeit wahrnehmen.

Big Data – Giant Data und Smartness

- Schätzungen zufolge hat die Menschheit gegenwärtig 17 Zettabyte (ZB) Daten produziert. 1ZB in Byte umgerechnet ergibt eine Eins mit 21 Nullen).

- Ende 2020: 69 Zettabyte

- Die Datenmenge steigt um 60% pro Jahr.
  (Vergleich: 2012: 50%)



http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode

„smarte“ Anwendungen nutzen Giant Data

- „smarte“ Anwendungen bedienen sich der Giant Data
- „smart“ – besonders kluge, pfiffige und intelligente Menschen, „Menschenwitz“
- Die „Smartness“ teilen wir uns nun mit Algorithmen. In der Annahme, die Algorithmen könnten menschliches Verhalten errechnen = vorhersagen, werden sie „intelligent“ genannt.

Was weiß mein „smartes“ Auto über mich?

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

Verbrauch, Füllstände

Schaltverhalten des Automatikgetriebes, Einspritzverhalten des Motors

Navigationsziele,

Bewegungsprofil,

Remote Ortung

Geräte- und Kartenkennungen

Fahrverhalten bei Glätte

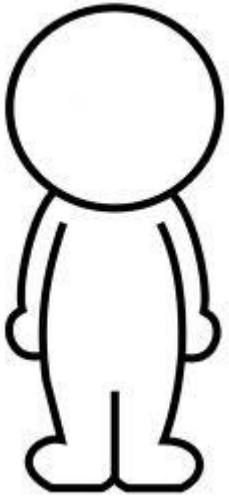
Fahrverhalten bei Nässe

Lautstärke Musik

Sensor-Daten, Aktuator-Daten

USA: event data recorder

Durchschnittsgeschwindigkeit, Einzelgeschwindigkeit verbunden mit Geodaten



E-call (EU) Telefonnummer

Sitzeinstellung

Adressbuch des Telefons, personalisierter Zugriff auf Dienste Dritter

Fehlerspeicher Anzahl Fehlfunktionen

Reaktionszeit auf Anzeigen

…

Smart Cars fahren in Smart Cities

<u>Smart Cities, „intelligente Städte“:</u>

- Smart Mobility, „intelligente Mobilität“
- Smart Prizes, „intelligente Preise“
- Smart Grids, „intelligentes Stromnetz“
- Smart Bosses, „kluge ArbeitgeberInnen“
- Smart Health, „intelligente Gesundheit“
- Smart Surveillance, „intelligente Überwachung“
- …

Riesige Möglichkeiten der **Profilbildung**

Grundrechtseingriff durch Smarte Anwendungen

ZEIT ONLINE: Sie sagen, Big Data sei eine Revolution. Warum?

Viktor Mayer-Schönberger: Weil es verändert, wie wir Wirklichkeit wahrnehmen.

Die auf der Profilbildung beruhenden Prognosen der Algorithmen verändern unsere Wahrnehmung der Realität (und die unserer Gegenüber). Sie greifen in die informationelle Selbstbestimmung ein.

Smartness und informationelle Selbstbestimmung

Was bedeutet das?

Titelbild des 37. Jahresberichtes der bremischen LfDI, Gestaltung: Marco Seifert

Beispiel Kreditscoring

Auch für die Entscheidung, wem Kreditinstitute etwa das „smart car“ finanzieren, gibt es „smarte“ Algorithmen:

Kreditscoring (= Algorithmus, der die Wahrscheinlichkeit errechnet, mit der eine Person einen Kredit vertragsgemäß bedienen wird.)

- Die Person wird einer Vergleichsgruppe zugeordnet, für die mit Hilfe eines statistisch-mathematischen Analyseverfahrens errechnet wird, mit welcher Wahrscheinlichkeit sie Kredite vertragsgemäß bedienen wird.
- Je mehr Datenarten für die Bildung der Vergleichsgruppen herangezogen werden,

  je mehr Vergleichsgruppen gebildet werden,

  je größer die Übereinstimmung zwischen den Daten der Person mit den Daten der Vergleichsgruppe ist,

  desto „smarter“, intelligenter, wird die Verhaltensprognose.

Grundrechtliche Anforderungen an “smarte” Algorithmen

Vermeidung personenbezogener Daten

- **Verzicht** – keine **personenbezogenen** Daten erheben (Datenminimierung, Artikel 5 Absatz 1 c DSGVO „Dem Zweck angemessen und erheblich sowie auf das für die Verarbeitung notwendige Maß beschränkt“)
- **Anonymisierung** – ursprünglich vorhandene **Personenbeziehbarkeit** nachträglich **verhindern** (Legaldefinition § 3 VI BDSG; Erwägungsgründe 26 ff DSGVO)

inhaltliche Anforderungen

- Rechtsgrundlage Einwilligung oder Gesetz (§ 28 b BDSG, Art. 22 DSGVO)
- Transparenz (§§ 28 b, 34 II BDSG, u.a. Art. 12-15 DSGVO)
- Grundsatz der freien menschlichen Letztentscheidung (§ 6a BDSG, Art. 22 DSGVO)

Erschwerter Zugang zu personenbezogenen Daten

Techn.-organ. Maßnahmen (Verschlüsseln, sichere Übertragungswege, etc.)

Vermeidung personenbezogener Daten - Anonymisierung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

- **Anonymisieren** (= personenbezogene Daten derart verändern, dass sie nicht mehr personenbeziehbar sind)

- **<u>Keine</u>** Anonymisierung bei Reidentifizierbarkeit aufgrund einer Kumulation von Angaben (**Profilbildung)**

- **<u>Keine</u>** Anonymisierung, wenn bei Dritten vorhandenes **Zusatzwissen** vorhanden ist, das eine Identifikation erlaubt

Bild gemorpht vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein

Grundrechtliche Anforderungen an “smarte” Algorithmen

Vermeidung personenbezogener Daten

- Verzicht – keine personenbezogenen Daten erheben (Datenminimierung, Art. 5 I c DSGVO)
- Anonymisierung – ursprünglich vorhandene Personenbeziehbarkeit nachträglich verhindern (Legaldefinition § 3 VI BDSG)

Inhaltliche Anforderungen

- Rechtsgrundlage Einwilligung oder Gesetz (§ 28 b BDSG, Art. 22 DSGVO)
- Transparenz (§§ 28 b, 34 II BDSG, u.a. Art. 12-15 DSGVO)
- Grundsatz der freien menschlichen Letztentscheidung (§ 6a BDSG, Art 22 DSGVO)

Erschwerter Zugang zu personenbezogenen Daten

Techn.-organ. Maßnahmen (Verschlüsseln, sichere Übertragungswege, etc.)

Inhaltlich Anforderungen - **Rechtsgrundlagen**

- **Greifen** Datenverarbeitungen in das Grundrecht auf informationelle Selbstbestimmung **ein**?

- Ist der **Eingriff gerechtfertigt** und daher **keine Verletzung** des Grundrechtes? Rechtfertigungsmöglichkeiten:

  1. **Einwilligung** der/des Betroffenen als Ausdruck der <u>individuellen</u> Selbstbestimmung
  2. **Gesetzliche Grundlagen** als Ausdruck der <u>kollektiven</u> Selbstbestimmung

Rechtsgrundlagen: **Einwilligung**

Art. 6 Absatz 1 Nr. a DSGVO
Wirksamkeitsvoraussetzungen nach Art. 7 DSGVO:

- **Freiwillig** (Abs. 4)
- **Informiert** (Abs. 2)
- Nachweisbar (Abs. 1)
- Jederzeit **widerruflich** (Abs. 3)
- Vor der Datenverarbeitung (Art. 6 Abs. 1 a)
- Für jede Verarbeitung und jeden Verarbeitungszweck (Art. 6 Abs. 1a)

Fehlt eine der Wirksamkeitsvoraussetzungen, liegt keine den Eingriff rechtfertigende Einwilligung vor.

Rechtsgrundlagen: **Gesetze**

- Europäische Ebene: z.B. ab Mitte 2018 Europäische Datenschutzgrundverordnung, z.B. **Artikel 22 Profiling**
- Bundesebene: z.B. bis Mitte 2018 **§ 28 b Bundesdatenschutzgesetz**
- Landesebene

Rechtsgrundlagen für Scoring: **Drei Daten-verarbeitungsschritte**

1. Aufbau des Datenbestandes

   Einwilligungen, Gesetzliche Grundlagen, §§ 28 ff Bundesdatenschutzgesetz

2. Bildung der Vergleichsgruppen aus dem Datenbestand

- Vorherige **Anonymisierung**
- Keine Anonymisierung bei Reidentifizierbarkeit aufgrund der Kumulation von Angaben (Profilbildung)
- Keine Anonymisierung, wenn bei beliebigen Dritten vorhandenes Zusatzwissen vorhanden ist, das eine Identifikation erlaubt

3. Zuordnung der Person zu einer der Vergleichsgruppen

   Art 22 DSGVO, § 28 b BDSG

Artikel 22 Datenschutz-grundverordnung

„1. Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich **Profiling** – beruhenden **Entscheidung unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

2. Absatz 1 gilt **nicht**, wenn die Entscheidung

(a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen **erforderlich** ist oder

->nicht einschlägig, da mildere Mittel als Nutzung von Scoringergebnissen denkbar sind

(b) aufgrund von **Rechtsvorschriften** der Union oder der Mitgliedstaaten, denen der für die Verarbeitung Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften **angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person** enthalten oder

-> § 28 b? Aus Sicht der Grundrechte strengere gesetzliche Voraussetzungen für Scoring erforderlich

(c) mit ausdrücklicher **Einwilligung** der betroffenen Person erfolgt. (…) “

Scoring, § 28b Bundes-datenschutzgesetz

„Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen **darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen <u>erhoben</u> oder verwendet werden**, wenn

1. (…)
2. (…)
3. (…)
4. (…).“

Aussagen des EuGH und gesetzliche Grundlagen für Profiling (1)

Deuten darauf hin, dass nach dem Europäischen Gerichtshof schon die **Profilbildungen selbst grundrechtlichen Beschränkungen unterworfen werden müssten**.

Urteil zu **Google-Spain**:

grundlegende Erwägungen zur Rolle des Internets, von Suchmaschinen und mit ihnen möglichen Profilbildungen in der modernen Gesellschaft

Allen, die diese Möglichkeiten nutzten, sei ein strukturierter Überblick über die zu Personen im Internet zu findenden Informationen möglich, die potenziell zahlreiche Aspekte von deren Privatleben betreffen könnten und ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden könnten.

Hieraus schließt der Europäische Gerichtshof, **wegen seiner potenziellen Schwere könne ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse an der Datenverarbeitung gerechtfertigt werden**.

Aussagen des EuGH und gesetzliche Grundlagen für Profiling (2)

Urteil zur **Ungültigkeit der Vorratsdatenspeicherungsrichtlinie**: Der Gerichtshof misst dem Grundsatz der **Erforderlichkeit** eine hohe Bedeutung bei. Auch die Aussagen zu technischen Anforderungen können auf Profilbildungen übertragen werden. Es sei entscheidend, dass es hinreichende Garantien gebe, dass die Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang und jeder unberechtigten Nutzung geschützt seien.

Im Urteil zur **Ungültigkeit der Safe-Harbor-Entscheidung**: Der Europäische Gerichtshof formuliert eine **strikte Zweckbindung** von Datenverarbeitungen, die **verletzt sei, wenn eine Regelung generell die Speicherung aller personenbezogenen Daten sämtlicher Personen gestatte.**

In Randnummer 91 bringt der Gerichtshofs seine ständiger Rechtsprechung folgendermaßen auf den Punkt: Eine Unionsregelung, die einen Eingriff in die durch die Artikel 7 und 8 der Charta garantierten Grundrechte enthalte, müsse **klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen** und Mindestanforderungen aufstellen, so dass die Personen, deren personenbezogene Daten betroffen seien, über ausreichende Garantien verfügten, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichten.

Grundrechtliche Anforderungen an “smarte” Algorithmen

Vermeidung personenbezogener Daten

- Verzicht – keine personenbezogenen Daten erheben (Datenminimierung, Art 5 I c DSGVO)
- Anonymisierung – ursprünglich vorhandene Personenbeziehbarkeit nachträglich verhindern (Legaldefinition § 3 VI BDSG)

Inhaltliche Anforderungen

- Rechtsgrundlage Einwilligung oder Gesetz (§ 28 b BDSG, Art. 22 DSGVO)
- **Transparenz** (§§ 28 b, 34 II BDSG, u.a. Art. 12-15 DSGVO)
- Grundsatz der freien menschlichen Letztentscheidung (§ 6a BDSG, Art. 22 DSGVO)

Erschwerter Zugang zu personenbezogenen Daten

Techn.-organ. Maßnahmen (Verschlüsseln, sichere Übertragungswege, etc.)

Inhaltliche Anforderung
Transparenz – § 28 b BDSG

„Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens **nachweisbar** für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens **erheblich** sind,
2. (…)
3. (…)
4. (…) “

Warum ist es für die Beurteilung des Kreditzahlungsverhaltens einer Person erheblich, wo sie wohnt, wie alt sie ist, welches Geschlecht sie hat, etc.?

Ausstellung „eyalter“ im Science-Center „Universum“ in Bremen; www.eyalter.com

Transparenz - § 28 b BDSG (2)

Anforderung nach § 28 b Nr. 1 Bundesdatenschutzgesetz:

Nachweis der Erheblichkeit der Daten, die unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen zur Berechnung des Wahrscheinlichkeitswerts genutzten werden.

Die Richtigkeit der **Annahmen**, die **dem Algorithmus zugrunde liegen** (etwa „ältere Menschen zahlen Kredite zuverlässiger zurück als jüngere Menschen“) muss nach § 28 b Nr. 1 BDSG **nachweisbar** sein.

Dies kann nur beurteilt werden, wenn die **Annahmen transparent** sind.

Transparenz – § 34 II BDSG

Auf das Scoring bezogener Auskunftsanspruch:

„(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1.die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,

2.die **zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten** und

3.das **Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte** einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.“

Transparenz – § 34 II BDSG nach Auslegung des Bundesgerichtshofes

- Schufa-Urteil des **BGH**: Transparenz gilt nur für Wissen, welche Daten gespeichert sind, nicht für „die Gewichtung einzelner Berechnungselemente bei der Ermittlung des Wahrscheinlichkeitswertes und die Bildung etwaiger Vergleichsgruppen“
- Aber die Argumentation ist widersprüchlich. Auszug aus dem Urteil:

  „(…) Denn dem Betroffenen soll – nicht zuletzt nach dem Willen des Gesetzgebers die Möglichkeit an die Hand gegeben werden, die in das Scoringergebnis eingeflossenen Lebenssachverhalte (…) nachzuvollziehen (…) und gegenüber der über eine Kreditvergabe entscheidenden Stelle bestimmte **Abweichungen** - etwa in der Kredithistorie – plausibel **durch bei ihm vorliegende <u>atypische</u> Lebenssachverhalte erklären** zu können.“
- Dies hat zur Voraussetzung, dass die Annahme, welcher Lebenssachverhalt vom Algorithmus als **<u>typisch</u>** zugrunde gelegt wird, bekannt ist.
- Transparenz muss sich danach auch auf die dem Algorithmus zugrunde liegenden Annahmen beziehen.

Transparenz - Grundrechtecharta

Artikel 8 Europäische Grundrechtecharta

„Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. **Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten** und die Berichtigung der Daten zu erwirken.“

Der Transparenzaspekt ist Bestandteil des Europäischen Grundrechtes.

Transparenz– Art. 13, 15 Datenschutz-grundverordnung

Art. 13 Absatz 2, Art 15 Absatz 2 Datenschutzgrundverordnung:

„Zusätzlich zu den Informationen gemäß Absatz 1 stellt der für die Verarbeitung Verantwortliche der betroffenen Person (…) folgende weitere Informationen zur Verfügung (…)“

13 Absatz 2 (f) bzw. 15 Absatz 2 (h):

„das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 20 Absätze 1 und 3 und – **zumindest** in diesen Fällen – **aussagekräftige Informationen über die involvierte Logik** sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.“

Enthält ebenfalls Forderung nach Transparenz über die dem Algorithmus zugrunde liegenden Annahmen.

Transparenz – Verbraucherschutz-ministerInnen

Beschluss der Verbraucherschutzministerkonferenz „Transparenz und Grenzen von Scoring-Verfahren gesetzlich sichern“

„(…) bedarf es dringend einer umfassenden Überarbeitung des Auskunftsanspruchs in § 34 BDSG, damit die Betroffenen überhaupt wirksame Maßnahmen zum Schutz ihrer allgemeinen Persönlichkeitsrechte ergreifen können“ (8.5.2015)

Transparenz für Smarte Algorithmen

Die europäischen und nationalen Grundrechte und Rechtsgrundlagen garantieren **Transparenz** darüber, welche unserer Daten in die Algorithmen eingespeist werden und welche Annahmen den Algorithmen zugrunde liegen. Die Transparenz darüber wird auch dazu beitragen, Vorurteile der **Algorithmen** zu beseitigen und sie damit **smarter** zu machen.

Quelle: http://www.betriebsratspraxis24.de/betriebsratspraxis-extra/typische-fehler-bei-der-betriebsratsarbeit/transparenz/

Anforderungen des Grundrechts auf informationelle Selbst-bestimmung an “smarte” Scorings

<u>Vermeidung personenbezogener Daten</u>

- Verzicht – keine personenbezogenen Daten erheben („Datenminiminerung“, Art. 5 I c DSGVO)
- Anonymisierung – ursprünglich vorhandenen Personenbezug nachträglich verhindern

<u>Inhaltliche Anforderungen</u>

- Rechtsgrundlage Einwilligung oder Gesetz (§ 28 b BDSG, Art. 22 DSGVO)
- **Transparenz** (§§ 28 b, 34 II BDSG, u.a. Art. 12-15 DSGVO)
- **Grundsatz der freien menschlichen Letztentscheidung** (§ 6a BDSG, Art. 22 DSGVO)

<u>Erschwerter Zugang zu personenbezogenen Daten</u>

Techn.-organ. Maßnahmen (Verschlüsseln, sichere Übertragungswege, etc.)

Inhaltliche Anforderung – freie menschliche Letzentscheidung

Grundsatz der freien menschlichen Letztentscheidung (§ 6a BDSG, Art. 22 DSGVO) – hier geht es um die menschliche „Smartness“

- **Menschliche** Letztentscheidung: Grundrechtsrelevante konkrete Einzelfallentscheidungen müssen von Menschen getroffen und verantwortet werden, denn wirklich „smart“ und „intelligent“ können nur Menschen sein.
- **Freiheit** der menschlichen Entscheidung: Diese Menschen dürfen keine Nachteile erleiden, wenn sie den „Vorschlägen“ des Algorithmus nicht folgen.

… bevor es zu philosophisch wird:

Europäische Datenschutzgrund-verordnung und Smartness

http://fs.cs.uni-frankfurt.de/artikel/don%C2%B4t-panic

Unser Schutz …

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Freie Hansestadt Bremen

Internetvertrauensbildende Maßnahme:

Die Europäische Grundrechtecharta

Titelbild des 38. Jahresberichtes der bremischen LfDI, Gestaltung: Marco Seifert

Gibt es noch Fragen an mich?

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Dr. Imke Sommer
Arndtstraße 1
27570 Bremerhaven
Tel. 0421/ 361-2010
E-Mail: office@datenschutz.bremen.de
www.datenschutz.bremen.de