Mag. iur. Dr. techn. Michael Sonntag

Übung Datenschutz

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

© Michael Sonntag 2012

Cookies

- Was ist ein Cookie?
  - → Kleine (max. 4 kB) Textdatei mit Informationen
  - → Inhalt (mit Beispielsdaten):
    - » Name: "session-id"
    - » Wert: "028-3057779-9388524"
    - » Domain: ".amazon.de"
    - » Webseiten-Pfad: "/"
    - » Ablaufdatum: 8.11.2006, 23:59:05
    - » Sicher (https): *
- Problem: Die Daten können irgend etwas sein
  - → Ein Teil davon ist ev. die IP-Adresse
  - → Oder auch bloß eine eindeutige Nummer

Cookies

- Sind Cookies "personenbezogene Daten"?
  - → Wann/Wann nicht?
- Erfüllung der Informationspflicht?
  - → Konkludente Zustimmung?
- In AGBs/Datenschutzerklärung ausreichend?
- Third-party Cookies
  - → Website x.at setzt Cookie für y.at
    - » x.at kann es selbst nicht auslesen
    - » Datenübermittlung an y.at (welche?)!
  - → Option "Accept cookies for originating site only"

Logging

- Logs sind sehr vielfältig:
  - → Weblogs: Server/Proxy
  - → Maillog
  - → Traffic-Log
  - → DHCP-Log
  - → Security-Logs
  - → …
- Personenbezug dieser Logs?
- Aber: Technische Überwachung ist nötig
  - → Wieweit? Welche Details? "Überwiegendes Interesse"?
  - → Wer hat Zugriff darauf?
  - → Spätere Verwendung zur Arbeitskontrolle?

Logging: Beispiele

- Webserver Log:
  - → 192.168.1.1 - - [03/Aug/2005:09:05:00 +0200] "GET / HTTP/1.1" 200 7277
- Mailserver Log:
  - → Nov 2 10:48:22 firewall sendmail[29980]: kA29mlo6029980: from=<someone@xyz.de>, size=225534, class=0, nrcpts=1, msgid=<4549CCCA02000008000BD3B2@oesnwgwn03.xyz.lan>, proto=ESMTP, daemon=MTA, relay=mail.xyz.de [192.168.1.1]
    Nov 2 10:48:37 firewall mimedefang.pl[11148]: MDLOG,kA29mlo6029980,mail_in,,,<someone@xyz.de>,<recipient@msv.at>,Antw: AW: Brief
  - → Nov 2 10:32:40 firewall pop3[29412]: login: [192.168.1.1] *someUserName authMethod* User logged in

Hausbesorgerdaten im Internet

- Veröffentlicht werden auf einer Webseite:
  - → Vorname, Nachname, Adresse, Telefonnummer, Zuständigkeitsbereich
- Klägerin ist Hausbesorgerin
  - → Ehemann: Chefinspektor der Polizei (Suchmittel und Waffen)
  - → Der Haushalt besitzt keinen Internet-Anschluss!
- Beklagter ist ein Sub-Unternehmer der Hausverwaltung
  - → Dieser hat die Homepage erstellt und veröffentlicht
  - → Die Hausverwaltung hat dem zugestimmt
    - » Sie wollte ohnehin schon länger eine Internet-Präsenz!
- Klagebegehren:
  - → Unterlassung der Veröffentlichung personenbezogener Daten im Internet

Hausbesorgerdaten im Internet

- Fragen zum Überlegen:
  - → Ist das ein Problem des Namensrechts?
  - → Um welche Art von Daten handelt es sich?
    - » Öffentliche Daten?
    - » Indirekt personenbezogene Daten?
    - » Sensible Daten?
  - → Ist es wichtig, dass der Ehemann besonders gefährdet ist?
  - → Wäre das Ergebnis anders, wenn die Klägerin selbst eine E-Mail Adresse/Homepage hätte?
  - → Definieren Sie das Interesse des Beklagten!
  - → Definieren Sie das Interesse der Klägerin!
    - » Müssen wir das überhaupt?
  - → Wozu überhaupt diese Definitionen?

Hausbesorgerdaten im Internet

- Fragen zum Überlegen:
  - → Was ist der Unterschied zwischen
    - » Schwarzem Brett im Stiegenaufgang
      - – Variante: Schwarzes Brett außen an der Eingangstür
    - » Homepage im Internet

- Variante: Eine Firma veröffentlich die Namen von Mitarbeitern, inkl. deren (Firmen-)Telefonnummer/E-Mail und ihrem Aufgabenbereich
    - » Beispiele: Putzfrau, Direktorin der Innenrevision, Sekretärin
  - → Wie wäre das zu beurteilen?
  - → Und was wäre mit einer Privat-Handy Telefonnummer?

Anmeldung beim DVR

- Standard vs. Musteranwendung
  - → Standard: Keine Meldepflicht
  - → Muster: Vorausgefülltes Formular
- Vergleich zu Adresshandel
  - → Was darf hier an Daten weitergegeben werden?
  - → Warum ist das hier erlaubt?
- Wie erfährt man von Standardanwendungen, wenn diese nicht gemeldet werden müssen?

Beispiel Standardanwendung
SA 22: Kundenbetreuung und Marketing

Zweck: Verwendung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.

Höchstdauer zulässiger Aufbewahrung: Die Daten dürfen bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Auftraggeber aufbewahrt werden.

3 Gruppen von Betroffenen:

- → Eigene Kunden, Interessenten, die an den Auftraggeber selbst herangetreten sind
- → Kontaktpersonen beim Kunden oder Interessenten
- → Potenzielle Interessenten; von Adressverlagen zugekauft (gemietet) oder selbst ermittelt

2 Empfängerkreise:

- → Adressverlage und Direktwerbeunternehmen gem. § 151 GewO 1994
- → Konzernleitung bei gewerblichen Kunden und Großkunden

Daten (Nur Auswahl!):

- → Name, Titel, Anrede, Geschlecht, Anschrift, Telefon, Fax, E-Mail, Sperrkennzeichen, Untersagung der Übermittlung an Adressverlage, Branchenbezeichnung, Geburtsdatum, Familienstand, Interessen, Kaufkraftklassifizierung, Betreuungsdaten, Kaufverhalten (Frequenz und Volumen), Antwortverhalten, Bonus-/Vorteilsdaten, …

Beispiel Musteranwendung: MA002: Zutrittskontrollsysteme

- **Zweck der Datenanwendung:**
  - → Kontrolle der Berechtigung des Zutritts zu Gebäuden und abgegrenzten Bereichen durch den Eigentümer oder Benutzungsberechtigten mit Hilfe von Anlagen, die personenbezogene Daten automationsunterstützt ermitteln und speichern, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.
- Betroffene Personengruppen: Zutrittsberechtigte
- Datenarten:
  - → Ordnungsnummer
  - → Bereichsspezifisches Personenkennzeichen; Personalverwaltung (PV)
  - → Vor- und Familienname, akad. Grad/Standesbezeichnung
  - → Geschlecht
  - → Beziehung des Betroffenen zum Auftraggeber (Mitarbeiter, Kunde, Besucher)
  - → Telefon-, Faxnummer, und andere zur Adressierung erforderliche Informationen, die zur raschen Verständigung des Betroffenen erforderlich sind
  - → Lichtbild des Betroffenen, sofern als zusätzliche Sicherheitsmaßnahme erforderlich
  - → Zutrittscode
  - → Vom Berechtigten einzugebender Berechtigungscode
  - → Daten der Zutrittsberechtigung, insbesondere Bereiche und Zeiten
  - → Gültigkeitsdauer der Zutrittsberechtigung

Weitergabe an Stammzahlenregisterberhörde erlaubt

Datensicherheitsmaßnahmen

REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION
DVR: 0000027
Stand: 1. August 2004

Datenverarbeitungsregister
A-1010 Wien, Hohenstaufengasse 3
Tel. (01) 531 15 / 4043
Fax: (01) 531 15 / 4016
E-Mail: dvr@dsk.gv.at

Allgemeine Angaben zu ergriffenen Datensicherheitsmaßnahmen
(gemäß Anlage 4 DVRV 2002 BGBl. II Nr. 24/2002)

1. Registernummer
(bitte eintragen, falls eine solche bereits zugeteilt wurde)

DVR:

2. Name (sonstige Bezeichnung) des Auftraggebers:

3. Bezeichnung der Datenanwendung:

Kreuzen Sie bitte in den nachstehenden Rubriken an, welche Datensicherheitsmaßnahmen Sie für die gemeldete Datenanwendung getroffen oder nicht getroffen haben. Soferne von Ihnen vorgesehene Datensicherheitsmaßnahmen in der Auflistung nicht angeführt sind, geben Sie bitte unter „Sonstige“ an, welche Datensicherheitsmaßnahmen Sie für die gegenständliche Datenanwendung getroffen bzw. zusätzlich getroffen haben.

4. Folgende Datensicherheitsmaßnahmen wurden für diese Datenanwendung ergriffen / nicht ergriffen: (Zutreffendes bitte ankreuzen ☒)

	JA	NEIN	
1.	☐	☐	Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern wurde ausdrücklich festgelegt;

Datensicherheitsmaßnahmen

	JA	NEIN	
1.	☐	☐	Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern wurde ausdrücklich festgelegt;
2.	☐	☐	die Verwendung von Daten wurde an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden;
3.	☐	☐	jeder Mitarbeiter wurde über seine nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt;
4.	☐	☐	die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters wurde geregelt und Maßnahmen gegen den Zutritt Unbefugter ergriffen;
5.	☐	☐	die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt;
6.	☐	☐	die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert;
7.	☐	☐	es wird Protokoll geführt, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können;
8.	☐	☐	es wird eine Dokumentation über die nach Z 1. bis 7. getroffenen Maßnahmen geführt, um die Kontrolle und Beweissicherung zu erleichtern.
9.	☐		Sonstige Datensicherheitsmaßnahmen:

Verdeckte Videoüberwachung

- Klägerin: Kassiererin in einem Getränkemarkt
  - → Fristlos gekündigt wegen Verdacht der Unterschlagung!
- Beklagter: Der Getränkemarkt
  - → Der frühere Arbeitgeber der Klägerin

- Klagebegehren:
  - → Feststellung, dass die Kündigung unwirksam war
  - → Lohn hierfür abzüglich erhaltenem Arbeitslosengeld
- Zugrunde liegende Frage: Durfte die Videoüberwachung stattfinden, und falls nicht, führt dies zu einem Beweisverwertungsverbot?

Verdeckte Videoüberwachung

- Fragen zum Überlegen:
  - → Was ist ein "Beweisverwertungsverbot"?
    - » Welche Beispiele gibt es dafür?
  - → Warum wollte der AG überhaupt per Video überwachen?
    - » Hätte es eine "gelindere" Maßnahme gegeben?
  - → Wie sieht es aus mit Grundrechten? Wer hat welche?
  - → Vergleich zu Beweisverwertungsverbot in den USA!
- Zusatz: Was ist mit der Datenschutzverletzung?
  - → Wird die Firma deswegen verurteilt?
- Variante: Videoüberwachung bei der Post
  - → Wie sieht es in diesem Fall mit der Abwägung aus?

Videoüberwachung: Beispiel

- Siehe die beiden Dateien:
  - → Begleitschreiben
  - → Meldungsformular
- Quelle: LVA an der FH Joanneum Datenschutz
  - → Abgabe von Herrn Christian Klingbacher

Überwachung am Arbeitsplatz

- E-Mail und Web-Nutzung:
  - → Warum will ein AG dies überhaupt überwachen?
  - → Dürfen AN überhaupt diese Dinge privat nutzen?
  - → Was ist mit trotzdem privaten Elementen?
    - » Beispiel: Privatanruf/Privat-E-Mail von außen?
  - → E-Mails: Gilt das Briefgeheimnis?
  - → Vorlage-Anweisung bei Firmenbriefen vs. Mithören bei Firmen-Telefonaten
- Was darf man daher als AG mit E-Mails machen?
  - → Vollautomatische Virensuche überhaupt ein Problem?
  - → Wie ist es mit SPAM?
- Wie sähe es bei betrieblichen Chats aus?
- Und ist eine Videoüberwachung erlaubt?
  - → Was ist z.B. mit den Banken (Kassa!)?

Adresshandel

- Wer darf mit Adressen Handel treiben?
- Was braucht man vom Kunden an "Erlaubnis"?
- Der Datenkatalog:
  - → Name, Geschlecht, Titel, Akad. Grad, Anschrift, Geburtsdatum, Berufs-/Branchen-/Geschäftsbezeichnung, Listenzugehörigkeit
  - → Welches Datum ist hier "gefährlich"?
    - » In welche Datenkategorie gehören diese Informationen?
  - → Und was ist mit anderen Daten:
    - » Erheben aus Kundendateien?
    - » Selbst sammeln?
    - » Abgeleitete Daten?

Herold Marketing-CD

- CD mit Informationen über (alle) österreichischen Haushalte
  - → Nur Daten über Konsumenten
  - → Nur verfügbar für Unternehmen (Gewerbeschein!)
- Enthält berechnete (=Statistik) Tiefendaten für Einzelpersonen
  - → Haushaltsvorstand
  - → Anzahl Personen/Kinder pro Haushalt
  - → Haushaltstyp
  - → Altersklasse
  - → Stellung im Haushalt
  - → Kaufkraftklasse
    - » Beispiel: Wird aus folgenden Elementen berechnet:
      = Altersklasse+Titel+Anschrift+Wohnsituation+statistische Daten

Herold Marketing-CD

- Fragen zum Überlegen:
  - → Woher stammen die Daten?
  - → Wie werden die "geschätzten" Daten berechnet?
  - → Wie ist das mit dem Grundsatz der "Daten-Korrektheit"?
  - → Welchem Zweck dient die CD?
  - → "Und wenn ich keine Aktualisierung (mehr) mache, dann lese ich die CD einfach direkt aus!"
  - → Kann man sich gegen die Aufnahme in die CD wehren?
    - » Kann man sich gegen die berechneten Daten wehren?
    - » Sollte man sperren oder löschen lassen?

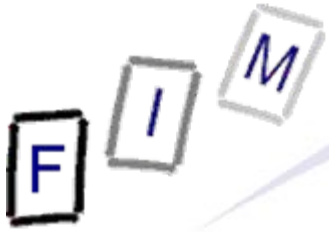
Herold Marketing-CD

- Prüfung durch die DSK erfolgte
- Ergebnis: Bericht mit "Empfehlungen"
  - → Keine Suche nach Einzelpersonen erlaubt
  - → Löschungspflichten müssen erfüllt werden
    - » Konsequenz: Verpflichtendes Update alle 3 Monate
    - » Ansonsten funktioniert die Software nicht mehr!
  - → Keine Daten(-kategorien) erlaubt, die unverhältnismäßigen Eingriff in Privatsphäre darstellen
    - » Problem ev.: Partnerschaftsverhältnis
      - – Haushaltstyp: Single, Verheiratet, Lebensgemeinschaft
      - – Zwei Männer + "LG" → Sensible Daten!

Friends of Merkur

- Klägerin: Verein für Konsumenteninformation
- Beklagte: Merkur AG

- Klagebegehren:
  - → Unterlassung der Verwendung best. AGB-Klauseln
  - → Urteilsveröffentlichung in der Kronen-Zeitung

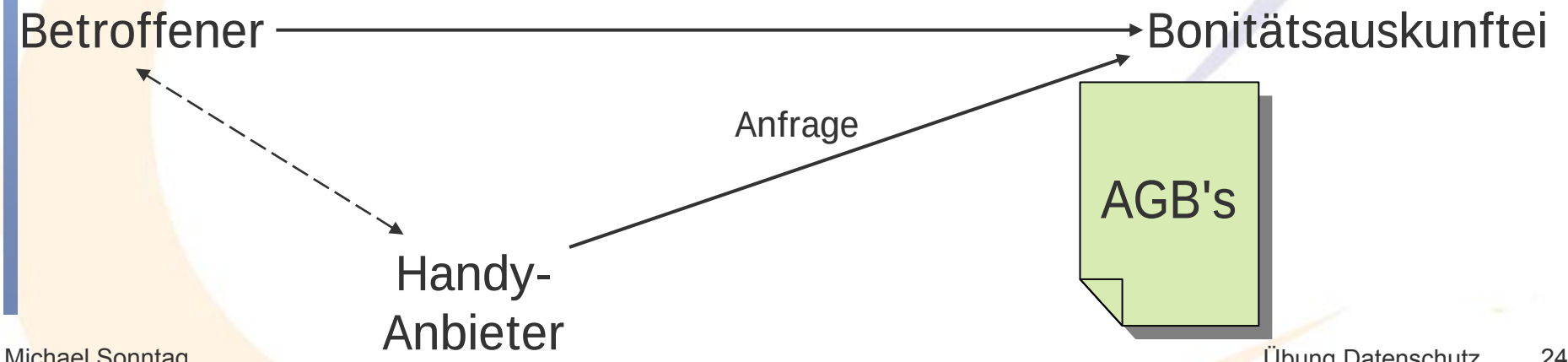


Friends of Merkur

- Fragen zum Überlegen:
  - → Warum klagt hier der VKI (hat der bei Merkur eingekauft)?
  - → Wie sind die AGBs auszulegen, falls unklar?
  - → Unterliegt der Fall dem KSchG?
    - » Es geht hier ja nicht um die einzelnen Kaufverträge!
  - → Wie ist das mit der Änderung der AGB's?
    - » Existieren hier Einschränkungen?
  - → Wer bekommt die Daten der Mitglieder?
  - → § 18 Abs 1 DSG (ALTE Fassung!): "ausdrückliche schriftliche Zustimmung" für Datenübermittlung nötig
    - » Heute: (bloße) Zustimmung
    - » Was sind "allfällige Werbemaßnahmen" (auch Telefon)?
  - → Wie weit haftet Merkur für Bankomatkarten-Missbrauch?
    - » Siehe § 6 Abs 1 Z 9 KSchG!

Bonitätsauskunfteien

- Klägerin: Ein (potentieller) Kunde eines Handyanbieters
  - → Vertrag wurde ihm verweigert, da es einmal eine Exekution gegen ihn gab
- Beklagte: Ein Bonitätsauskunftei
  - → Sammelt öffentliche Bonitätsdaten
- Klagebegehren:
  - → Löschung seiner Daten



Bonitätsauskunfteien

- Fragen zum Überlegen:
  - → Wer ist der Auftraggeber: Die Bonitätsauskunftei oder der Handy-Anbieter?
  - → Auf welche rechtliche Grundlage beruft sich der Kunde?
    - » Welche Voraussetzungen sind zu erfüllen?
  - → Ist eine Bonitätsauskunftei dieser Art "öffentlich"?
- Zukunft:
  - → Was ist die potentielle Folge dieses Urteils?
  - → Welche Abhilfsmöglichkeiten sind vorstellbar?
- Neuere Urteile:
  - → Händische Prüfung des Interesses im Einzelfall → OK!
    - » Dann ist die Datenbank nicht öffentlich
  - → Öffentlich + Widerspruch → Löschung
    - » Verschieben in internen Bereich geht dann nicht mehr
    - » Ev: Spätere Daten könnten intern + händische Prüfung bleiben

Bonitätsauskunfteien

- Gesetzliche Sonderregelung seit 6/2010
  - » § 7 Abs 5 Verbraucherkreditgesetz
  - → Registrierte Informationsverbundsysteme kreditgebender Institutionen zur Bonitätsbeurteilung sind vom Widerspruchsrecht nach § 28 Abs 2 DSG ausgeschlossen (§ 28 Abs 1 DSG gilt weiterhin!)
    - » Z.B. „Konsumentenkreditevidenz“ und „Warnliste der Banken“
  - → Löschung der Daten daraus also nur bei:
    - » falschen Daten
    - » rechtswidrig ermittelten Daten
    - » nicht aktuellen Daten
    - » überwiegenden berechtigten Interessen des Betroffenen
- Dies betrifft nicht die „Privaten“ Bonitätsauskunfteien
  - → Achtung: KKE&Warnliste werden vom KSV geführt, dieser ist aber nur Dienstleister für die Banken (=techn. Durchführung)

Bodil Lindqvist: Facts

- Miss Lindqvist works as a cleaning lady and in a church
- After a computer course she installed a homepage to inform all the church members on current events
  - → She initiated a link from Swedish church homepage to hers
- Content of the homepage
    - » About her and 18 work colleagues from the parish
  - → Complete name or only christian name
  - → Employment or hobbies
  - → Sometimes the family situation (married, …)
  - → Partly the telephone number
  - → For some persons further information
  - → One co-worker: She hurt her leg and is partially on sick leave
- There is no consent by these persons
  - → After some complaints the pages were removed immediately

Bodil Lindqvist: Procedure

- The public prosecutor started proceedings because of
  - → Automated processing of personal data without previous notification of the "Datainspektion"
    - » Datainspektion = The Swedish privacy commission
  - → Processing sensible data without prior permission
    - » Collecting and putting it in the webpage, publishing the webpage on a webserver
  - → Export of personal data to third countries without permission
    - » I.e., publishing on the Internet (accessible from everywhere)
- First instance: Penalty of ≈ € 450,-

Bodil Lindqvist: Questions

- What the Swedish supreme court asked the ECJ:
  - → Is mentioning the name of a person on a webpage a privacy matter? Is this "automated processing of personal data"?
  - → Is mentioning a leg injury/sick leave medical (=sensible) data?
  - → Is publishing on the Internet a transmission abroad?
    - – Swedish person puts Swedish data on a Swedish server
      - » Is it important whether some foreign person accessed it?
      - » Is it important where the server is located?
  - → Are the directive restrictions compatible with the ECHR?
  - → Can a country institute more stringent protection laws?

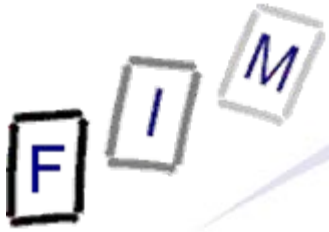
- Note:
  - → The facts are undisputed
  - → What is at issue is solely their legal evaluation!

Bodil Lindqvist: Aspects to consider

- What exactly is personal data?
  - → Where is the delineation to anonymous data?
  - → What of the data listed is "personal data"?
- What about purely personal data processing?
  - → What is it? Is it applicable here?
- When is data processing "automated"?
- What is data "concerning health"?
  - → Is this to be seen narrowly or extensively?
- When a web server is accessed from other countries, how does this happen technically?
  - → How technically exports the data?
  - → What is a physical comparison to this?

Bodil Lindqvist: Aspects to consider

- The EU is not (yet) member of the ECHR
  - → What about those rules? Are they applicable?
- What is "harmonization"?
  - → Does this mean that all countries must do the same?
  - → What's the difference between "directive" and "regulation"?
  - → Define the scope of the directive with regard to national laws!



Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

© Michael Sonntag 2012