Datenschutz

Grundlagen

Michael Sonntag

Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz, Austria

sonntag@fim.uni-linz.ac.at

Dienstleister

- Wie Auftraggeber, aber sie verwenden Daten nur zur Herstellung eines Werkes im Auftrag
  - Nicht: Werkvertrag! Kann jede beliebige rechtliche Konstruktion sein!
- Wichtiger Aspekt: Keine eigene Entscheidung, sondern nur die Durchführung der Entscheidung eines Anderen (=des Auftraggebers)
  - D.h., technischer Vorgang der Verwendung wird von jemand anderem ausgeführt (=Dienstleister) als demjenigen, der dies getan haben möchte (=Auftraggeber)
- Beispiel:
  - ISP verschickt Werbe-E-Mails an alle Kunden eines Unternehmens, die dem zugestimmt haben
    - Wird selbst zum Auftraggeber, wenn er eigene Werbung dranhängt!

Überlassen von Daten

- Die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses
  - Rechtlich „harmlos“, da der Zweck gleich bleibt
  - Ohne besondere Auflagen/Genehmigungen/… erlaubt
    - Sofern die Auftrags-Datenverwendung legal ist (dafür gibt es Anforderungen!)
- Beispiel:
  - Versandhandelsunternehmen gibt Adressen an Druckerei weiter, welche diese auf Briefe, Kuverts, … druckt
    - Nicht mehr Überlassung sondern Verarbeitung (und daher kein DL mehr sondern selbst Auftraggeber!): Speichern der Daten, um später selbst Werbung verschicken zu können

Informationsverbundsystem

- Gemeinsame Datenverarbeitung in einer Anwendung durch mehrere Auftraggeber
- Gemeinsame Benützung der Daten: Jeder kann auf alle Daten zugreifen
- Beispiel: Kleinkreditevidenz
  - Jede Bank speist ein, welche Personen welche Kredite haben
  - Jede Bank kann auf **alle** Kreditinformationen zugreifen
    - Also insbesondere auch auf die, welche andere Banken eingestellt haben!
- Kein Informationsverbundsystem: Lediglich technisch gemeinsam, aber jeder kann nur auf „seine“ Daten zugreifen
- Besonders gefährlich (weite Verbreitung der Daten, mehrere Zugriffsberechtigte): Darf daher erst nach Genehmigung der DSK betrieben werden!

Zustimmung

- Datenschutz ist zwar ein Grundrecht, aber disponibel
  - Dies bedeutet, man kann auch darauf verzichten
  - Eine Zustimmung in die Verwendung ist jederzeit möglich
- Die Zustimmung ist aber deutlich „schwieriger“ als sonst im Gesetz!
  - Erfordert drei separate Aspekte, die alle gegeben sein müssen:
    - Freiwilligkeit
    - Informiertheit
    - Konkretisierung
- Nicht erforderlich: Schriftlichkeit (aber: Nachweis!)

Zustimmung: Frei

- Kein Zwang oder Druck
  - Ablehnung eines Vertrags ist möglich, wenn keine Zustimmung erfolgt
    - Aber: Monopole (zB “alle Banken machen dies so”) ???
    - Praxis: Sehr viel ist hier möglich (Privatautonomie)
- Aber das ist doch immer Voraussetzung für einen Vertrag?!?
  - Daher ist hier „etwas mehr“ Freiheit nötig!
- Typisches Beispiel: Arbeitsvertrag
  - Im Arbeitsvertrag können (fast) beliebige Zustimmungen stehen
    - Jeder kann zustimmen oder die Arbeit ablehnen (Aber: Theorie! → AMS?)
  - Aber bei bestehendem Vertrag ist fast keine Zustimmung mehr möglich!
    - Arbeiter: „Sonst wirst du entlassen!“; Manager: Eher möglich!

Zustimmung: Informiert

- Information über folgende Punkte muss (vorher!) erfolgen
  - Dass personenbezogene Daten verwendet werden sollen
    - Link zu „Datenschutz-Policy“, Hinweis, …
  - Welche Daten verwendet werden sollen: „Wir werden IP-Adresse, Klicks, … sammeln“
  - Wozu die Daten verwendet werden sollen: Zweck
    - „Anpassung der Website an Benutzer-Bedürfnisse!
  - Wer der Auftraggeber ist: Siehe Impressum!
  - An wen die Daten übermittelt werden sollen (gegebenenfalls)
    - Genaue Bezeichnung (z.B. „Werden die Daten auch an die XYZ AG weiterleiten“)
- Besonders wichtig für implizite Zustimmung
  - Zustimmen kann man nur dem, worüber man informiert wurde!

Sonstige Informationspflichten

- Wenn es nach Treu und Glauben erforderlich ist, zusätzlich noch
  - Bestehen eines Widerspruchsrechts
    - Standardmäßig ist das nicht erforderlich
  - Rechtliche Verpflichtung zur Beantwortung oder nicht
    - Nur, wenn das nicht ohnehin klar erkennbar ist
    - Damit man weiß was passiert, wenn man nicht antwortet
    - Wichtig hauptsächlich für (halb-)staatliche Stellen/Erfüllung von Vorschriften!
  - Verarbeitung in einem Informationsverbundsystem ohne gesetzlich Anordnung
    - Damit man weiß, dass auch andere die Daten erfahren könnten

Zustimmung: Konkret

- Zustimmung ist nur für „einzelne“ Verwendungen möglich
  - Das kann auch eine lange Liste sein, aber keine generelle Zustimmung!
- Konkret bedeutet: Information muss „genau genug“ sein
  - Für einen bestimmten Zweck:
    - **NICHT** “wir können damit machen was wir wollen”
    - Wichtigster Teil! Aber auch keine absolut detaillierte Aufzählung nötig
      - Beispiel: „Werbezwecke" ist nicht konkret genug
      - „Bewerbung eigener Produkte" könnte ausreichen
  - Für bestimmten Auftraggeber/Empfänger
    - **NICHT** “Übermittlung an befreundete Unternehmen”

Wann dürfen Daten verwendet werden?

- Zweck und Inhalt der Verwendung müssen von den Befugnissen des Auftraggebers gedeckt sein
  - Nicht „einfach so“, sondern im Rahmen des Betriebes
- Schutzwürdige Geheimhaltungsinteressen der Betroff. dürfen nicht verletzt sein
  - Genaueres dazu separat für normale und sensible Daten geregelt!
- Minimalitätsprinzip ist zu berücksichtigen
  - Nur im erforderlichen Ausmaß
  - Mit den gelindesten Mitteln
  - Einhaltung der Grundsätze für die Verwendung von Daten

Wann dürfen Daten übermittelt werden?

- Sie müssen aus einer zulässigen Datenanwendung stammen
  - Die Verarbeitung an sich (siehe vorige Folie) muss legal sein
- Zweck und Inhalt der Übermittlung dürfen die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzen
- Empfänger hat Übermittelndem seine ausreichende Befugnis im Hinblick auf den Übermittlungszweck glaubhaft gemacht
  - Nachweis, dass Empfänger die Daten für den vorgesehenen Zweck verarbeiten darf
- Zustimmung? → Doppelt erforderlich!
  - Für diesen Zweck verarbeiten
  - Übermittlung an anderen, d.h. für neuen Zweck verarbeiten

Schutzwürdige GI: Normale Daten

- „Abschließende“ Aufzählung, d.h. diese sechs Fälle ermöglichen die Verwendung (aber nicht: Übermittlung!) nicht-sensibler Daten
  - 1: Ausdrückliche gesetzliche Ermächtigung oder Verpflichtung
    - Beispiel: Betriebe → Krankenstand der Mitarbeiter für Gehaltsabrechnung
  - 2: Zustimmung des Betroffenen
    - Widerruf ist jederzeit möglich und bewirkt Unzulässigkeit weiterer Verwendung
      - Achtung: Ein darauf aufbauender Vertrag kann dann ebenfalls wegfallen! Dann ist dies quasi ein jederzeitiges Kündigungsrecht!
  - 3: Lebenswichtige Interessen des Betroffenen erfordern dies
    - Nachprüfen in Datenbanken auf Medikamenten-Unverträglichkeiten

4: Überwiegende berechtigte Interessen Dritter

- Überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten
  - Öffnungsklausel: Jede beliebige Verwendung ist erlaubt, wenn sie entsprechend argumentiert werden kann!
- Praktische Bedeutung: Hoch
  - Berechtigtes Interesse: Normalerweise kein Problem (Umsatzsteigerung, … → ✓)
  - Überwiegen der Interessen: Knackpunkt!
- Aspekte der Interessensabwägung:
  - Darf keine rein monetäre Abwägung sein
    - Betroffener = - € 900, Auftraggeber = + € 1000 → Dennoch verboten
  - Liste im Gesetz (siehe unten) dient als Anhaltspunkt

Schutzwürdige GI: Strafrechtsbezogene Daten

- Strafrechtsbezogene Daten dürfen verwendet werden:
  - Zulässigerweise veröffentlicht oder nur indirekt personenbezogen: Wie oben!
  - Ausdrückliche gesetzliche Ermächtigung oder Verpflichtung: Wie oben!
  - Wesentliche Voraussetzung für einen Auftraggeber des öff. Bereichs für die Wahrnehmung einer gesetzlich übertragenen Aufgabe: Wie oben!
  - Zulässigkeit ergibt sich auch gesetzlichen Sorgfaltspflichten oder überwiegenden berechtigten Interessen des Auftraggebers und die Art und Weise der Verwendung wahrt die Interessen der Betroffenen
    - Berechtigte Interessen Dritter sind hier draußen (außer über Sorgfaltspflichten)!
    - Besondere Sicherheitsmaßnahmen, Zugriffsbeschränkungen etc. erforderlich

Schutzwürdige GI: Strafrechtsbezogene Daten

— Zweck ist die Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlung/Unterlassung zuständige Behörde

- Unzuständige Behörde → Datenschutzverletzung!
- Hintergrund: „Geheimnisverrat“ von (Ex-)Mitarbeitern, …
  - Verbotenes Verhalten anzuzeigen soll nicht gleichzeitig selbst eine Straftat sein → Würde viele davon abhalten, dies anzuzeigen!
- Wo eine Anzeigepflicht besteht: Siehe oben (Gesetzliche Verpflichtung)!

Verwendung für wiss. Forschung/Statistik

- Sind die Ergebnisse nicht personenbezogen, so dürfen alle Daten verwendet werden, die
  - Öffentlich zugänglich sind
  - Für andere Untersuchungen zulässigerweise ermittelt wurden
  - Für ihn nur indirekt personenbezogen sind
- Das heißt, sie dürfen personenbezogen verarbeitet werden, aber am Ende muss anonymisiert werden!
  - Stärker noch: Wenn gerade nicht/nicht mehr benötigt, muss sofort pseudonymisiert oder anonymisiert werden!
- Sonst: Besondere gesetzliche Vorschriften, Zustimmung der Betroffenen oder Genehmigung der Datenschutzkommission

Automatisierte Einzelentscheidungen

- Niemand darf einer vollautomatischen Entscheidung unterworfen werden, die rechtliche Folgen nach sich zieht oder ihn erheblich beeinträchtigt, wenn dies Aspekte seiner Person bewertet
  - Beispiele: Berufliche Leistungsfähigkeit, Bonität, Zuverlässigkeit
- Aber es gibt wichtige Ausnahmen von diesem Grundsatz!:
  - Ausdrücklich gesetzlich vorgesehen
  - Abschluss oder Erfüllung eines Vertrages und dies erfolgt auch
    - Vollautomatische Bonitätsprüfung ist OK, wenn der Kredit vergeben wird. Wenn nicht, muss eine manuelle Nachkontrolle erfolgen
  - Geeignete Maßnahmen wahren die berechtigten Interessen des Betroffenen
    - Beispiel: Er kann seinen Standpunkt gelten machen → Daher relativ wertlos!

Datensicherheitsmaßnahmen

- Datenschutz bringt nur dann etwas, wenn auch Datensicherheit gegeben ist
- Sicherheitsmaßnahmen müssen dem Stand der Technik entsprechen
- Der Auftraggeber muss die Daten sichern gegen
  - Zufälliger oder unrechtmäßiger Zerstörung, Verlust: Unveränderter Weiterbestand
  - Ordnungsgemäße Verwendung: Keine unerlaubte Datenverwendung
  - Zugriff Unbefugter: Geheimhaltung
- Durch technische und organisatorische Vorkehrungen
- Mitarbeiter müssen sich jederzeit darüber informieren können
  - Schriftlich, interner Webserver, …
- Auftraggeber ist verantwortlich; er muss Dienstleister entsprechend verpflichten!

Ausmaß des Schutzes

- Entsprechend dem Stand der Technik: Neue Technologien müssen sofort in Betracht gezogen werden
- Entsprechend der wirtschaftlichen Vertretbarkeit
  - Nicht alles was möglich ist, muss auch gemacht werden
- Sicherheitsniveau muss Art der Daten sowie Umfang und Zweck ihrer Verwendung entsprechen
  - Allgemeine Betrachtung: Wie „gefährlich“ wäre Weitergabe/Löschung/… der Daten für einen „typische“ Betroffene
    - Wenn Einzelpersonen in größerer Gefahr sind → Unbeachtlich!
- Ergebnis: Daten und Risiken analysieren, mit Sicherungsmethoden vergleichen
  - Und dann entsprechendes Niveau festlegen und umsetzen

Minimalanforderungen/Kategorien

- Aufgabenverteilung zwischen Organisationseinheiten/Mitarbeitern festlegen
- Verwendung von Daten an gültige Aufträge Anordnungsbefugter binden
- Mitarbeiterbelehrung über Datenschutz- und Datensicherheitsvorschriften
- Regelung der Zutrittsberechtigungen zu Räumlichkeiten
- Zugriffsberechtigungen auf Programme, Datenträger regeln
- Schutz von Datenträger vor Einsicht/Verwendung durch Unbefugte regeln
- Berechtigungen zum Betrieb der Datenverarbeitungsgeräte regeln und jedes Gerät gegen unbefugte Inbetriebnahme absichern
- Protokollierung tatsächlich durchgeführter Verwendungsvorgänge, damit ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden kann
- Dokumentation der getroffenen Maßnahmen für Kontrolle/Beweissicherung

Protokollierung

- Protokolle dürfen nicht für Zwecke verwendet werden, die mit der Zulässigkeitskontrolle unvereinbar sind
  - Insbesondere nicht zur Kontrolle der Personen, die auf die Daten zugegriffen haben
    - Außer um deren Zugriffsberechtigung zu prüfen
    - Aber zB nicht, um festzustellen, wann, wie oft, wie intensiv sie gearbeitet haben!
  - Ausnahme: Verhinderung oder Verfolgung eines Verbrechens >5 Jahre (Höchststrafe) Gefängnis oder wegen einer kriminellen Organisation (§ 278a StGB)
- Protokolle sind 3 Jahre lang aufzubewahren
  - Außer gesetzlich anders angeordnet (Steuer: 7 Jahre)
  - Abweichung möglich sofern Daten früher gelöscht oder länger aufbewahrt werden

Datengeheimnis

- Auftraggeber, Dienstleister und deren Mitarbeiter müssen Daten geheim halten
  - Wenn diese ihnen ausschließlich auf Grund der berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden
  - Ausnahme nur, wenn es eine legale Übermittlung ist (d.h., wenn Daten formell weitergegeben werden dürfen, darf man das auch entsprechend erzählen/…)
- Sonstige Verschwiegenheitspflichten gelten weiter (und unabhängig)
- Übermittlungen durch Mitarbeiter bedürfen einer ausdrücklichen Anweisung
- Mitarbeiter müssen vertraglich auf das Datengeheimnis verpflichtet werden
  - Steht üblicherweise im Dienstvertrag!
  - Belehrung über Verletzungsfolgen ist ebenso nötig

Dienstleister

- Der Einsatz von Dienstleistern ist grundsätzlich zulässig
  - Müssen aber ausreichend Gewähr für rechtmäßige und sichere Verwendung bieten
  - Dies muss vereinbart werden (=genaue Verpflichtung im Vertrag)
  - Über die tatsächlichen Maßnahmen muss sich der Auftraggeber informieren lassen
    - Pflicht, eine Dokumentation über alle Maßnahmen zu übergeben
- Vereinbarungen über die genaue Ausgestaltung der Dienstleister-Pflichten müssen zwecks Beweissicherung schriftlich erfolgen

Pflichten des Dienstleisters

- Datenverwendung ausschließlich im Rahmen der Aufträge
- Keine Übermittlung ohne Auftrag
- Alle erforderlichen Datensicherheitsmaßnahmen sind zu treffen
  - Nur Mitarbeiter heranziehen, die dem Datengeheimnis unterliegen
    - Dienstvertrag oder gesetzliche Verschwiegenheitspflicht (zB Ärzte)
- Weitere Dienstleister nur mit Billigung des Auftraggebers
  - So rechtzeitige Information, dass dieser das untersagen kann
- Technische und organisatorische Vorkehrungen, sodass Auskunfts-, Richtigstellungs- und Löschungspflicht erfüllt werden können
- Nach Dienstleistungsende alle Verarbeitungsergebnisse oder Unterlagen dem Auftraggeber übergeben oder in dessen Auftrag aufbewahren, oder vernichten

Vielen Dank für Ihre Aufmerksamkeit!

Michael Sonntag

Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz, Austria

sonntag@fim.uni-linz.ac.at