

Datenschutz

Grundlagen

Michael Sonntag

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz, Austria

sonntag@fim.uni-linz.ac.at

Grundrecht auf Datenschutz

- Geheimhaltung personenbezogener Daten, sofern ein schutzwürdiges Geheimhaltungsinteresse besteht
- Kein Geheimhaltungsinteresse, wenn
 - Allgemeine Verfügbarkeit der Daten
 - Jeder kann problemlos Zugang dazu erlangen (=öffentliche Daten)
 - Siehe aber später die Ausnahmen!
 - Mangelnde Rückführbarkeit auf den Betroffenen
 - Anonymisierte Daten

Wessen Daten sind geschützt?

- Natürliche Personen
 - Alle Menschen
 - Nicht: Tiere, Gegenstände (außer: In Bezug auf den Besitzer)!
 - Auch Kinder gegenüber Eltern (aber: Erziehungsrecht/-pflicht, ...)
 - Auch Mitarbeiter gegenüber dem Arbeitgeber
 - Auch Manager/Politiker/... gegenüber der Öffentlichkeit
- Juristische Personen
 - Firmen
 - International ungewöhnlich
 - Kommt aus der Vergangenheit (war in Ö schon immer so)
- Dies sind die „Betroffenen“

Welche Daten sind geschützt?

- Alle Daten in Bezug auf eine Person:
 - Beispiele: Haarfarbe, Stimme, Briefe, persönliche Gewohnheiten/Vorlieben, Einkommen, Sexuelle Orientierung, letztes Frühstück, Bonität, ...
 - Unabhängig davon, ob “wichtig” oder nicht
 - Kann mit anderen Daten zusammen wichtig werden
 - Jeder kann die Wichtigkeit (sehr weitgehend) für sich selbst bestimmen
- Ergebnis: Liste von “Personen” (wie auch immer identifiziert) und “Eigenschaft(en) dieser Person“ → Liste ist geschützt
 - Achtung: Verstecktes Datum!
 - “Auf der Liste stehen”, d.h. die Überschrift auf dem Zettel!

Wann sind Daten geschützt?

- Nur Daten die verwendet werden, aber nicht die Daten selbst (=“Faktum”)
 - Sammeln von Name + Haarfarbe → Datenschutz
 - Aber keine Einschränkungen durch den Datenschutz für die Haarfarbe selbst!
- Auch öffentliche Daten können geschützt sein
 - Insbesondere, wenn die Öffentlichkeit eingeschränkt ist
- Für einen Schutz durch das DSGVO müssen Daten
 - Automatisiert verarbeitet werden
 - Manuelle Verarbeitung: Landesgesetzgebung (Praktisch Abschriften des DSGVO!)
 - Besitzt heute nur mehr sehr wenig Bedeutung!
 - Manuelle Verarbeitung in Dateien und Gesetzgebung ist Bundessache

Wo gilt das Ö DSG?

- Wichtig wegen der el. Verarbeitung!
- Verwendung von Daten im Inland
 - „Verwendung“: Siehe später; umfassend!
- Verwendung von Daten im EU-Ausland für Zwecke einer in Ö gelegenen Haupt- oder Zweigniederlassung
 - Bsp: In Passau werden die Daten der Linzer Filiale verarbeitet
- Ausländisches Recht bei Verarbeitung in Ö:
 - Sitzstaat des Auftraggebers, wenn Private mit Sitz in der EU Daten in Ö verwendet, die keiner Ö Niederlassung des Auftraggebers zuzurechnen sind
 - Spiegelbild zu oben!
- Keine Anwendung, wenn bloße Durchfuhr

Ausschluss-Bereiche

- Von fast allen Betroffenen-Rechten ausgenommen (aber grundsätzlich dem Datenschutz unterliegend) sind folgende Datenverwendungen:
 - Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich
 - Alles, was in der Verfassung vorkommt: Nationalrat, Bundesrat, Landtage, ...
 - Sicherung der Einsatzbereitschaft des Bundesheeres
 - Stellungen-Listen, Bereitstellungs-Daten (Großmaschinen etc.)
 - Sicherung der Interessen der umfassenden Landesverteidigung
 - Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der EU
 - Vorbeugung, Verhinderung oder Verfolgung von Straftaten
 - Spezialregelungen in der Strafprozessordnung (Rechtsschutzbeauftragter, ...)!

Was sind (direkt) personenbezogene Daten?

- Daten über Betroffene, deren Identität bestimmt oder bestimmbar ist
 - Man weiß genau wer dies ist
 - Jemand können die Person irgendwie bestimmen
 - Absolute Identität ist nicht nötig, aber zumindest kleine Gruppe
 - „Josef Müller“ reicht ev. nicht, da es davon sehr viele gibt!
 - Gilt ganz allgemein, rein „Daten-bezogen“
- Dies sind „direkt“ personenbezogene Daten!
- Beispiel:
 - Name + Geburtsdatum + Bonität
 - Name (+ ev Geburtsdatum) → Genau bestimmt, wer dies ist

Was sind indirekt personenbezogene Daten?

- Indirekt personenbezogene Daten
 - Eine bestimmte Person kann den Personenbezug mit rechtlich zulässigen Mitteln nicht bestimmen
 - Mit illegalen ev schon!
 - Indirekt Personenbezogen: Gilt nur für eine bestimmte Person
 - Für andere ev direkt Personenbezogen!
- Beispiel:
 - Sozialversicherungsnummer + Gehalt
 - Für Studenten indirekt: Sozialversicherungsnummer kann nicht aufgelöst werden
 - Für Krankenkassen direkt: Besitzen Zugriff auf Liste (Name, SV-Nummer)
 - Für Arbeitgeber: Bei „seinen“ Angestellten direkt, bei anderen indirekt

Sensible Daten

- Besonders geschützte („gefährliche“) Daten
 - Sehr viel weniger damit erlaubt: Stärkere Einschränkungen
- Abschließende Aufzählung im Gesetz:
 - Rassistische/ethnische Herkunft: Hautfarbe
 - Politische Meinung: Parteizugehörigkeit/-naheverhältnis
 - Gewerkschaftszugehörigkeit: Vereinsmitgliedschaft bei entspr. Vereinen
 - Religiöse/Philosophische Überzeugung: Religionsbekenntnis, Atheist
 - Gesundheit: Krankheiten (Nicht: Schwangerschaft, Blutgruppe!)
 - Sexualeben: Bestimmte Vorlieben, sexuelle Orientierung

Auftraggeber

- Wer die Entscheidung getroffen hat, Daten zu verwenden
 - Egal ob sie es selbst machen oder jemanden damit beauftragen (→ Dienstleister)
 - Kann ein Einzelperson (nat./jur.) sein, eine Personengemeinschaft, Organe/Geschäftsapparate von Gebietskörperschaften
 - Egal ob die Entscheidung alleine oder gemeinsam getroffen wurde
 - Wichtiges Kriterium: Hier wird ein „Zweck“ festgelegt → Was erreicht werden soll
- Gilt auch dann, wenn Dienstleister selbst eine Entscheidung zur Verwendung für diesen Zweck treffen, außer
 - Dies wurde ihm ausdrücklich untersagt
 - Der Beauftragte hat aufgrund von Rechtsvorschriften oder Verhaltensregeln eigenverantwortlich über die Verwendung zu entscheiden

Verwenden von Daten

- Jeder Art der Handhabung von Daten
 - Was auch immer damit passiert, es ist „Verwenden“
- Inkludiert:
 - Verarbeiten: Selbst benützen
 - Überlassen: Technische Ausführung eigener Verarbeitung durch Dritte
 - Eigentlich Untergruppe von „Verarbeiten“!
 - Übermitteln: Weitergabe an Dritte
- Prinzipiell verboten, außer es ist explizit erlaubt
 - Allerdings gibt es sehr weitreichende Ausnahmen!

Verarbeiten von Daten

- Alles was mit Daten passiert, außer es wäre eine „Übermittlung“
 - Negative Definition!
- Beispiele:
 - Ermitteln, Erfassen: Schon die bloße Sammlung/Erfassung ist betroffen!
 - Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Sperren: Jegliches verarbeiten
 - Überlassen: An Dienstleister
 - Löschen, Vernichten: Auch die Entsorgung ist betroffen
 - Der Betroffene kann selbst ein Interesse am Fortbestand besitzen
 - Beispiel: Krankenakte
- Nicht: Übermittlung!

Übermitteln von Daten

- Weitergabe von Daten an andere Empfänger als Betroffenen, Auftraggeber oder Dienstleister
 - Insbesondere gehört hierzu das Veröffentlichen!
 - Auskunft an Betroffenen ist daher niemals eine Übermittlung und (fast) immer legal!
 - Auftraggeber \Leftrightarrow Dienstleister: Überlassen (siehe unten)
- Oder: Verwendung der Daten für anderes Aufgabengebiet des Auftraggebers
 - Jede Zweckänderung ist eine Übermittlung!
 - Daher auch Übermittlung von sich selbst zu sich selbst möglich!
 - Adresse für Warensendung \rightarrow Nutzung für Parteiwerbung \rightarrow Übermittlung
- Übermittlungen sind rechtlich „schwer“!

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
 - Zustimmung kann man nur dem, worüber man informiert wurde!

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

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 berechnigte Interessen Dritter

- Überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten
 - Öffnungsklausel: Jede beliebige Verwendung ist erlaubt, wenn sie entsprechend argumentiert werden kann!
- Praktische Bedeutung: Hoch
 - Berechnigtes 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: Normale Daten

- Schutzwürdige Geheimhaltungsint. werden bei der Verwendung nicht verletzt bei
 - 5: Zulässigerweise veröffentlichten Daten
 - „Zulässigerweise“ ist neu im Gesetz, d.h. ohne Zustimmung/sonst unerlaubt veröffentlichte Daten dürfen **nicht** verwendet werden!
 - Praxis: Wie soll das festgestellt werden? Sehr schwierig! Daher eher nur dann, wenn vom Betroffenen selbst veröffentlicht (da ist es klar zulässig)!
 - 6: Indirekt personenbezogenen Daten
 - Diese sind daher „Freiwild“ und dürfen beliebig verwendet werden
 - Achtung: „Veröffentlichung“ ist eine Übermittlung und daher potentiell umfasst
 - Diese Daten dürfen aber wohl dennoch nicht veröffentlicht werden, da sie für andere Personen ja direkt personenbezogen sind!

Überwiegende berechnigte Interessen

- Beispielhafte (!) Aufzählung im Gesetz
 - Was ähnlich ist, kann daher ebenfalls erlaubt sein
 - Wesentliche Voraussetzung für einen Auftraggeber des öff. Bereichs für die Wahrnehmung einer gesetzlich übertragenen Aufgabe
 - Damit man das nicht in jedes Gesetz hineinschreiben muss
 - Darf keine bloße Erleichterung, sondern muss „erforderlich“ sein
 - Durch Auftraggeber der öff. Bereichs in Erfüllung von Amtshilfe
 - Wenn es eine andere Behörde unbedingt braucht
 - Zur Wahrung lebenswichtiger Interessen Dritter
 - „Lebenswichtig“ = Wirklich wichtig (neues Auto anbieten → ✗, suche nach geeigneten Blutspendern, um diese zu Fragen → ✓)

Überwiegende berechnigte Interessen

- Erfüllung vertraglicher Verpflichtung zwischen Auftraggeber und Betroffenen
 - ZB Verarbeitung der Adresse für die Zusendung von Waren
 - Ansonsten könnte man dies als Rücktrittsrecht benützen!
 - Voraussetzung: Vertrag! Geht daher erst nachher, nicht bei der Prüfung, ob überhaupt ein Vertrag abgeschlossen werden soll.
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig und Daten wurden rechtmäßig ermittelt
 - Gerichte sind hier ebenfalls Behörden
 - Datenschutz soll Rechtsdurchsetzung nicht behindern
 - Rechtmäßige Ermittlung → Keine Verwendung illegal erlangter Daten
 - Illegale Aufzeichnungen (Video, Audio, ...)

Schutzwürdige GI: Sensible Daten

- **Abschließende** Aufzählung im Gesetz
 - Das heißt, keine Generalklausel/Interessensabwägung!
 - Was nicht auf der Liste steht (oder sonst explizit in diesem/einem Gesetz), geht nicht!
- Geheimhaltungsinteressen werden ausschließlich dann nicht verletzt, wenn
 - Betroffener die Daten offenkundig selbst öffentlich gemacht hat
 - Wer die eigenen Daten veröffentlicht, gibt sein Geheimhaltungsinteresse auf
 - Beispiel: „Coming-out“ von Homosexuellen, aber nicht deren (Fremd-)„Outing“!
 - Die Daten nur indirekt personenbezogen verwendet werden
 - Keine Gefahr, da ja keiner Person zuordenbar
 - Auch hier nur „Verwendung“, d.h. keine Übermittlung/Veröffentlichung!

Schutzwürdige GI: Sensible Daten

- Ermächtigung oder Verpflichtung durch gesetzliche Vorschriften
 - Achtung: Keine Verordnung, Bescheid etc → Gesetz!
 - Gesetz muss zusätzlich noch einem **wichtigen** öffentlichen Interesse dienen
 - Normale Daten: „Öffentliches Interesse“. Daher hier viel enger!
- Durch Auftraggeber der öff. Bereichs in Erfüllung von Amtshilfe
 - Wie oben, wird nach der anfordernden Behörde beurteilt
- Betrifft ausschließlich die Ausübung einer öffentlich. Funktion durch den Betroffenen
- Ausdrückliche Zustimmung des Betroffenen
 - Auch hier ist ein Widerruf jederzeit möglich
 - Aber: Ausdrücklich → Keine konkludente Zustimmung mehr möglich
 - Nicht jedoch: Schriftlich oder sonstige Formvorschrift!

Schutzwürdige GI: Sensible Daten

- Verarbeitung oder Übermittlung ist zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig und dessen Zustimmung kann nicht rechtzeitig eingeholt werden
 - Bei sensible Daten kann man für sich selbst ablehnen → Lieber sterben!
- Verwendung der Daten ist zur Wahrung lebenswichtiger Interessen Dritter notwendig
 - Bei anderen kann man nicht ablehnen ...
 - Dafür gibt es hier auch keine Übermittlung, sondern nur „Verwendung“
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig und Daten wurden rechtmäßig ermittelt
 - Wie bei normalen Daten!
- Besondere Ausnahmen: Private Zwecke, Wiss. Forschung und Statistik, Benachrichtigung/Befragung Betroffener oder Katastrophenfall

Verwendung für private Zwecke

- Natürliche Personen dürfen für ausschließlich persönliche oder familiäre Tätigkeiten Daten verarbeiten, wenn
 - Diese vom Betroffenen selbst mitgeteilt wurden
 - Sie ihnen sonst rechtmäßigerweise zugekommen sind (Übermittlung)
- Diese Daten dürfen für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden
 - D.h., sie müssen im privaten Bereich bleiben!
- Beispiel:
 - Bekannten-Liste wird verwendet, um diesen Versicherung anzubieten
 - Übermittlung aus dem private Bereich hinaus → Verboten!

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

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

Rechte der Betroffenen

- Als Betroffener erhält man mehrere Rechte:
 - Auskunftsrecht: Was passiert, welche Daten sind über mich gespeichert
 - Jeder: Durchgeführte Standardanwendungen
 - Betroffene: Alle, wo sie darin vorkommen
 - Richtigstellung: Falsche Daten berichtigen/bestreiten
 - Löschung: Illegal verwendete Daten müssen gelöscht werden
 - Widerspruchsrecht: Opt-out aus der Datenverwendung
 - Wegen besonderer Geheimhaltungsinteressen
 - In besonderen Fällen einfach so
- Keine Geltendmachung möglich, wenn Daten nur indirekt personenbezogen verwendet werden (auch wenn man die Identifikation ermöglicht!)

Auskunft

- Jeder Person ist Auskunft über deren verarbeitete Daten zu geben
 - Antrag muss schriftliche erfolgen und die eigene Identität nachweisen
 - Mit Zustimmung des Auftraggebers auch mündlich
 - Mit Zustimmung des Betroffenen auch bloße Einsicht + Abschrift/Ablichtung
 - Keine Daten → Negativauskunft ist dennoch verpflichten
- Mitwirkungspflicht im Verfahren, zB Kundennummern etc. bekanntgeben
- Auskunft binnen 8 Wochen nach Einlagen, oder schriftl. Ablehnungs-Begründung
- Ab Kenntnis des Verlangens dürfen die Daten 4 Monate lang nicht gelöscht werden (bei Beschwerde an DSK bis zu deren rechtskräftigem Abschluss)
 - Außer wenn der Betroffene einen Löschungsantrag stellt

Auskunft

- Auskunft ist unentgeltlich
 - Aktueller Datenbestand und ein Mal pro Jahr
 - Sonst Pauschale von € 18,89 oder tatsächliche höhere Kosten
 - Rückerstattung bei Richtigstellung oder Löschung!
- Auskunftsanfrage an Dienstleister → Weiterleitung an Auftraggeber
 - Plus Mitteilung, dass er keine Daten verwendet (das macht rechtlich der Auftraggeber!)
- Informationsverbundsysteme: Ein Betreiber ist zu bestellen
 - Betreiber muss binnen 12 Wochen Auskunft erteilen, wer von jemandem der AG ist
- Geschäftsgeheimnisse können als Einschränkung dienen
 - Und werden oft vorgebracht!

Richtigstellung/Löschung

- Falsche (Inhalt!) Daten sind zu korrigieren, illegal verarbeitete Daten zu löschen
 - Sobald die Unrichtigkeit/Unzulässigkeit bekannt wird
 - Auf begründeten Antrag des Betroffenen
- Richtigstellung fällt weg, wenn dies für den Verarbeitungszweck irrelevant ist
 - Potentielles Problem bei Übermittlungen → Beim Ziel-Zweck ev. von Bedeutung!
- Unvollständigkeit ist nur dann ein Fehler, wenn das Gesamte dadurch im Hinblick auf den Zweck unrichtig wird
 - Kein Anspruch auf Hinzufügung beliebiger Daten!
- Sobald Daten für den Zweck nicht mehr benötigt werden, wird wie Verarbeitung unzulässig und sie sind zu löschen (außer: Archivierung)

Richtigstellung/Löschung

- Beweis der Richtigkeit der Daten: Auftraggeber!
 - Außer: Gesetz / Ausschließlich aufgrund von Angaben des Betroffenen erhoben
- Keine Richtigstellung/Löschung, wenn dies Dokumentationszweck widerspricht
 - Dann sind Anmerkungen zu machen (Beispiel: Krankenakte)
- Antrag ist binnen 8 Wochen zu erfüllen und dies dem Betroffenen mitzuteilen
 - Ansonsten in selber Frist eine schriftliche Begründung (Erfüllung: Auch elektronisch!)
- Löschung wegen Wirtschaftlichkeit nur zu bestimmten Zeitpunkten möglich
 - Sperrung + berichtigende Anmerkung (Typ. Beispiel: Rollendes Backup)
- Richtigkeit nicht feststellbar: Bestreitungsvermerk ist anzubringen
 - Löschung nur mit Betroffenen-Zustimmung oder wegen Entscheidung von Gericht/DSK

Widerspruch

- Wenn die Verwendung nicht gesetzlich vorgesehen ist, kann man Widerspruch einlegen, wenn man überwiegende Geheimhaltungsinteressen besitzt
 - „Allgemein ist das kein Problem, aber für mich ist das gefährlich(er) als für Andere“
 - Muss sich aus der besonderen Situation des Betroffenen ergeben
 - Löschung binnen 8 Wochen und keine Übermittlungen mehr
- Öffentlich zugängliche Datenanwendung ohne gesetzliche Anordnung
 - Jederzeitiger Widerspruch auch ohne Begründung (anders als oben!)
 - Löschung binnen 8 Wochen
- Siehe spezielles dazu im Teil über Bonitätsprüfungen!

Rechtsdurchsetzung

- Geteilt zwischen DSK und Zivilgerichten
- DSK:
 - Öffentlicher Bereich (Verwaltung)
 - Auskunftsrecht, Automat. Einzelentscheidungen
 - Kontrollbefugnisse für alle Datenanwendungen
- Zivilgerichte:
 - Geheimhaltung, Richtigstellung, Löschung, Widerspruch
- Akte der Gesetzgebung oder Gerichtsbarkeit: Keine Durchsetzung möglich
 - Gerichte: Innerhalb des Instanzenzuges möglich
 - Gesetzgebung (Parlamentarische Ausschüsse!): Gar nichts

Strafbestimmungen: Gericht

- Komplexer Vorsatz erforderlich
 - Unrechtmäßige Bereicherung von sich selbst oder einem Dritten
 - Oder einen anderen im Geheimhaltungsanspruch zu schädigen
 - Daten wurden ausschließlich auf Grund der berufsmäßigen Beschäftigung anvertraut oder zugänglich oder wurden widerrechtlich verschafft
 - Daten werden benützt, zugänglich gemacht oder veröffentlicht
 - Schutzwürdiges Geheimhaltungsinteresse des Betroffenen
 - Keine Bestimmung mit strengerer Strafe
- Freiheitsstrafe bis zu einem Jahr

Strafbestimmungen: Verwaltung

- Drei Varianten: Verletzung, Gefährdung, Verzögerung
 - Bereits der Versuch ist strafbar
 - Verfall von Datenträgern/Geräten kann angeordnet werden
 - Zuständig: Bezirksverwaltungsbehörde des Sitzes des Auftraggebers
- Verletzung: Es ist tatsächlich etwas passiert → € 25.000
 - Vorsätzlich widerrechtlichen Zugang verschaffen oder erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhalten
 - Vorsätzliche Übermittlung entgegen Datengeheimnis (= auch Zweckänderung!)
 - Daten entgegen Urteil/Bescheid verwendet, nicht beauskunftet/richtigstellt/löscht
 - Vorsätzlich löscht (bei Auskunftsbegehren oder Gericht/DSK-Verfahren)
 - Unter Vortäuschung falscher Tatsachen vorsätzlich Daten beschafft, wie dies für den Katastrophenfall vorgesehen ist

Strafbestimmungen: Verwaltung

- Gefährdung: Noch ist nichts passiert, aber Gefahr steigt → € 10.000
 - Ermitteln, verarbeiten übermitteln, ohne Meldepflicht erfüllt zu haben
 - Datenanwendung abweichend von der Meldung betreiben
 - Daten ins Ausland ohne DSK-Genehmigung übermittelt oder überlässt
 - Gegen Zusagen an die oder Auflagen von der DSK verstößt
 - Verletzung der Offenlegungs- oder Informationspflichten
 - Gröbliche Außerachtlassung der erforderlichen Sicherheitsmaßnahmen
 - Nicht-Löschung der Daten einer Videoüberwachung nach Zeitablauf
- Verzögerung: € 500
 - Auskunft, Richtigstellung, Löschung, Widerspruch nicht binnen der Frist erfolgt

DSG-Novelle: Geplante Änderungen

- Einführung eines freiwilligen Datenschutzbeauftragten
 - Keine Meldepflicht mehr, nur mehr ein Verzeichnis, wer wen als DSB bestellt hat!
- Vorabkontrolle nur mehr bei sensiblen Daten und Daten zur Bewertung einer Person
 - Entfällt: Videoüberwachung, Informationsverbundsysteme, Strafrechts-Daten, in Gesetzen oder Verordnungen geregelt und DSK "genehmigt" diese, Verwendung mit ausdrücklicher Zustimmung des Betroffenen
- Vereinfachte Standardanwendungen
- Erledigung von Altverfahren (die jetzt nicht mehr gemeldet/... werden müssten)
- (Inoffizieller!) Hauptgrund: Unterfinanzierung/Unterbesetzung des DSK

Zusammenfassung

- Datenschutz ist wichtig, aber wird oft als nicht wichtig angesehen
 - Datenschutz = Täterschutz → Oft zitiert, fast immer falsch!
 - Wenn nicht: Auch die StPO ist Täterschutz!
 - Die Polizei darf nicht einfach beliebige Räume durchsuchen!
- Praktische Durchsetzung in Österreich: Extrem schwach!
- Wichtig:
 - Gute Argumente finden, da bei „normalen“ Daten die Interessensabwägung wichtig ist
 - Bei Heranziehung von Dienstleistern vorsichtig sein: Umfassende Verträge/Informationen sind erforderlich (Einmal gemacht → Dann nur mehr kleines Problem!)
 - Bei der SW-Herstellung gleich auf DS achten (Betroffenen-Rechte, Protokollierung)
 - Besonders acht geben, wenn Daten ins Ausland „wandern“, egal wie

Vielen Dank für Ihre Aufmerksamkeit!

Michael Sonntag

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)

Johannes Kepler Universität Linz, Austria

sonntag@fim.uni-linz.ac.at