Datenschutz und Signaturverfahren

Jan Skrobotz

30.09.2004

Datenschutz und Signaturverfahren

Grundlagen — Signaturverfahren — Chancen — Gefährdungen

- Datenschutz: Die Grundlagen

  Art. 1_I und 2_I GG, Art. 10 GG, Art 13 GG, BVerfGE 65,1

- Anforderungen an Signaturverfahren

  Bundes-Datenschutzgesetz BDSG, § 14 SigG

- Chancen der Signaturverwendung

  Datensparsamkeit als Ziel: Pseudonyme

- Gefährdungen durch Signaturen

  Gefahr des „Personenkennzeichens“

Datenschutz und Signaturverfahren

- keine Geheimwissenschaft, sondern Balance der Interessen
- effektive Verwaltung & Datenverarbeitung vs. „totale Kontrolle“
- Historie: Großrechner, Personenkennzeichen, „Big Brother“
  - Unbehagen angesichts unbegreiflicher Datenverwendung in leistungsfähigen Großrechnern und Datenbanken
  - Gefahr der Verknüpfung aller aggregierter Daten
  - 1970er Jahre: das Personenkennzeichen im Melderegister, Gesetzgebung zum Bundes-Datenschutzgesetz 1976
  - „renitenter“ Rechtsausschuss kippt Meldegesetz

Datenschutz und Signaturverfahren

- Masse an dem Staat bekannten Daten:
  - BKA: Vorstrafen, Ermittlungsdaten
  - Sozialversicherung: Rentenerwartung, Vorleben
  - Polizei: Bußgelder, Ermittlungen
  - Grundbuchamt, Baubehörde: Bautätigkeit, Wirtschaftsdaten, Eigentum
  - Krankenhaus, Gesundheitsamt, Krankenkasse: Krankheiten, Arzneimittel
  - Bundeswehr: Musterungsdaten, Beurteilungen, Waffen
  - Gerichte: Vorstrafen, Gerichtsakten, Scheidungsakten
  - Schulamt, ZVS: Zeugnisse, Noten
  - Arbeitsamt: Berufsleben, Löhne und Gehälter
  - Kfz-Bundesamt: Auto, Verkehrsverstöße
  - Sozialamt: Einkommen, Schulden, Unglücksfälle
  - Kommunen: Wählerlisten, Parteienlisten, politisches Verhalten
  - Bibliotheken: Lesegewohnheiten
- Großes Interesse der Wirtschaft an all diesen Daten

Datenschutz und Signaturverfahren

- Gefahr der Verknüpfung all dieser Daten,
  Gefahr der Profilbildung, des gläsernen Bürgers,
  Gefahr des Missbrauchs
- besonders: das Personenkennzeichen als eindeutige Nummer, die eine Verknüpfung erheblich erleichtert – alle Parteien sprachen sich gegen eine solche Verknüpfungsmöglichkeit aus
- keine Regelung, bis 1983: Das Volkszählungsurteil des BVerfG („BVerfGE 65, 1“)
- Datenverwendung als grundrechtsrelevante Staatstätigkeit?

Datenschutz und Signaturverfahren

- simples Prüfschema des BVerfG:
  - Grundrecht, Schutzbereich
  - Eingriff
  - Rechtfertigung
- zwei wichtige Grundrechte: Art. 10_I und Art. 13_I GG

  Art. 10 Abs. 1 GG: Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

  Art. 13 Abs. 1 GG: Die Wohnung ist unverletzlich.

  „unverletzlich“: Eindringen, Lauschen, Schauen sind als Eingriff verboten und bedürfen der Rechtfertigung

Datenschutz und Signaturverfahren

- Was aber ist mit rechtmäßig erlangten Daten? Analogie?
- zwei andere Grundrechte: Art. 1_I und Art. 2_I GG

  Art. 1 Abs. 1 GG: Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

  Art. 2 Abs. 1 GG: Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit ...

- Aus der Würde des Menschen folgt sein Recht, selbst über sein Leben zu entscheiden, sein Selbstbestimmungsrecht, auch in informationeller Hinsicht.

Datenschutz und Signaturverfahren

- Das Grundrecht gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden.“
- Der Bürger muss wissen können, „wer was wann und bei welcher Gelegenheit über ihn weiß.“
- Wer sich beobachtet glaubt, und Aufzeichnung fürchtet, wird sich angepasst verhalten, und seine Grundrechte nicht nutzen.
- Datenerhebung, -speicherung, -auswertung und -verwendung sind Eingriffe in dieses Recht (Stufe 2 der Prüfung)
- besonders intensiv: elektronische Datenspeicherung, da diese rasches Auffinden und „Data Mining“ ermöglicht

Datenschutz und Signaturverfahren

- Rechtfertigung (Stufe 3): abhängig vom Grundrecht
  - Art. 1 GG: Die Würde des Menschen ist unantastbar.
    „unantastbar“ bedeutet: eine Rechtfertigung ist nicht möglich, jeder Eingriff ist per se verboten
  - Art. 2 GG: ... soweit er nicht ... gegen die verfassungsmäßige Ordnung ... verstößt.
    „verfassungsmäßige Ordnung“: jedes verfassungsgemäß zustandegekommene Gesetz
- Also: Rechtfertigung durch verhältnismäßiges Gesetz möglich, solange die Datenverwendung nicht die Menschenwürde verletzt (keine „Herabwürdigung zum Objekt staatlichen Handelns“)

Datenschutz und Signaturverfahren

- wesentlicher Aspekt: *verhältnismäßiger* Eingriff
  - Geeignetheit (zielführend — „Hilft das überhaupt?“)
  - Erforderlichkeit (geringstmöglich — „Geht's nicht anders?“)
  - Verhältnismäßigkeit i. e. S. („Ist das nicht übertrieben?“)
- im Zentrum steht meist die *Erforderlichkeit* —
  denn häufig *geht* es eben auch anders, weniger einschneidend
- speziell in Bezug auf Daten: keine unnötige Erhebung, keine unnötige Speicherung, keine unnötige Verknüpfung, kein unnötiger Austausch, keine unnötige Offenbarung
- am besten: Datensparsamkeit

Datenschutz und Signaturverfahren

- diese Grundsätze gelten auch für Private —
  der Staat ist insoweit Gewährsträger
- Normierung in der EU-Datenschutzrichtlinie 95/46/EG,
  im Bundes-Datenschutzgesetz BDSG
  und in Spezialgesetzen, etwa § 14_{I} SigG, § 10_{II} SigG
- § 3a BDSG: Datensparsamkeit
  Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
- § 4 Abs. 1 BDSG: Zulässigkeit der Datenverwendung
  Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Datenschutz und Signaturverfahren

- § 14 Abs. 1 SigG, Datenschutz:
  Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.

- Zentralbegriff: „personenbezogene Daten“
  - jedes Datum, das einen Bezug zu einer konkreten Person ermöglicht, direkt oder indirekt („Halter des Autos B-CD 123“)
  - nur wahrhaft anonyme Daten sind nicht personenbezogen
  - bei Pseudonymen *kann* der Personenbezug hergestellt werden, wenn man das verknüpfende Datum kennt

Datenschutz und Signaturverfahren

- Prinzipien des Datenschutzes:
  Transparenz, Erforderlichkeit, Zweckbindung
- Einwilligung als „Idealziel“: Maximale Transparenz,
  Freiheitsverwirklichung durch Willensbetätigung
- Grundprinzipien
  - strikte Zweckbindung, keine „Vorratshaltung“
  - Erforderlichkeit für diesen Zweck, Löschung bei Zweckwegfall
  - Transparenz: Erhebung beim Betroffenen, Auskunftsrecht
  - Datensicherheit = Schutz vor Ausspähen und Missbrauch
  - Schutz vor falschen Daten: Berichtigungsanspruch

Datenschutz und Signaturverfahren

- „Zertifizierungsdiensteanbieter“
  - sonst im Signaturgesetz nur „angezeigte“ Anbieter qualifizierter Zertifikate
  - hier wegen § 14 Abs. 3 SigG jeder Aussteller von Zertifikaten, auch haus- oder vereinsinterne Zertifizierungsstellen
- „Betroffener“
  - jede Person, dessen Daten der Zertifizierungsdiensteanbieter erhebt, speichert, verarbeitet
  - in erster Linie der Signaturschlüssel-Inhaber, doch auch etwa der Vertretene oder zustimmende Stellen

Datenschutz und Signaturverfahren

- Zweckbindung: „für Zwecke eines qualifizierten Zertifikates“
  - notwendig sind daher alle Daten, die in ein Zertifikat gehören, § 7 SigG
  - und alles, wozu das Signaturgesetz den Anbieter verpflichtet, bspw. Dokumentation nach § 10 SigG
  - ebenso aber die Daten, die für‘s Geschäft wichtig sind: Vertrags- und Kontodaten
- Erforderlichkeit
  - ausgerichtet am Zweck; Speicherung eher als Veröffentlichung
  - Löschung bei Zweckwegfall: Aufbewahrungsfristen der § 10 SigG und §§ 4, 8 SigV — grundsätzlich fünf Jahre

Datenschutz und Signaturverfahren

- Transparenz
  - direkte Erhebung beim Betroffenen / Erhebung bei Dritten
  - Auskunftsanspruch, § 10 Abs. 2 SigG
    Dem Signaturschlüssel-Inhaber ist auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.
  - Verhältnis zu § 34 BDSG ist ungeklärt, v. a. die Rechte Dritter, und die Kostenfreiheit (§ 34 Abs. 5 BDSG)
- Datensicherheit
  - § 10 SigG Abs. 1 verlangt Schutz der Daten vor Veränderung
  - Verschlüsselungspflicht gemäß der Anlage zu § 9 BDSG
  - Berichtigungsanspruch ist nicht ausdrücklich normiert, § 20 Abs. 1 BDSG als Auffangnorm

Datenschutz und Signaturverfahren

- Pseudonyme Signaturen: Datensparsamkeit als Ziel
  - Pseudonyme sind nicht unmittelbar personenbezogene Daten
  - Sinn der Datensparsamkeit: Wo personenbezogene Daten nicht erhoben werden, bestehen keine Risiken, muss die Datenverwendung nicht reguliert werden
- Pseudonyme Zertifikate: § 5 Abs. 3 SigG

  [1]Der Zertifizierungsdiensteanbieter hat auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat an Stelle seines Namens ein Pseudonym aufzuführen. [2]Enthält ein qualifiziertes Zertifikat Angaben über eine Vertretungsmacht für eine dritte Person oder berufsbezogene oder sonstige Angaben zur Person, ist eine Einwilligung der dritten Person oder der für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle zur Verwendung des Pseudonyms erforderlich.

Datenschutz und Signaturverfahren

- Problem: Wer verlässt sich auf eine Unterschrift von „H. H. Ausgelacht“?
  - im Geschäftsverkehr: wer bei Problemen sein Geld bekommt
  - bei Banken: niemand
    (daher im 1. SigÄndG geplant: die Ergänzung von Satz 1 oben, „soweit vertraglich nichts anderes bestimmt ist“)
  - im Behördenverkehr: niemand
    („Sozialhilfe für Dagobert Duck“)

Datenschutz und Signaturverfahren

- Streit um die Aufdeckbarkeit eines Pseudonyms: § 14 SigG

  (2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat der Zertifizierungsdienste-anbieter die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies [...] erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen ...

- das heißt: Kein eigenständiges Aufdeckverfahren für Private
  - Gesetzgeber: zu leichte Aufdeckung entwertet Pseudonyme
  - „im Rahmen anhängiger Verfahren“: Wie verklagt man ein Pseudonym? Klagen müssen zugestellt werden, § 253 ZPO.
  - allenfalls: „anhängige“ Verfahren, nicht „rechtshängige“
  - gerade Datenschützer beklagen die hiesige restriktive Haltung
  - in Österreich ist eine Aufdeckung möglich, § 18 $_{\text{I \#3}}$ öDSG

Datenschutz und Signaturverfahren

- Irrelevanter Streit?
  - wer nicht mag, akzeptiert Pseudonyme auch bei Aufdeckbarkeit nicht, Banken z. B.
  - ohnehin: Bonität / Liquidität wichtiger als Identität: Kredit- und Pre-Paid-Karten
  - bei geringwertigen Gütern sind „Streuverluste“ hinnehmbar
  - bei höherwertigen Gütern sind die Transaktionskosten eines Medienbruchs unerheblich
  - bei langfristigen Vertragsbeziehungen sind Pseudonyme hinderlich, jedenfalls aber ist ihr Effekt dann minimal

Datenschutz und Signaturverfahren

- keine Pseudonyme im Behördenverkehr: § 87 a Abs. 3 und 4 AO

  (3) [1]Eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. [2]In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. [3]Die Signierung mit einem Pseudonym ist nicht zulässig.

  (4) [1]Eine durch Gesetz für Verwaltungsakte oder sonstige Maßnahmen der Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. [2]In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. [3]Für von der Finanzbehörde aufzunehmende Niederschriften gilt Satz 1 nur, wenn dies durch Gesetz ausdrücklich zugelassen ist.

- „Wo kämen wir denn da hin!“
  - das Finanzamt darf Pseudonyme verwenden, Bürger nicht
  - „Der Fiskus weiß ohnehin alles. Schutz? Steuergeheimnis!“

Datenschutz und Signaturverfahren

- keine Pseudonyme im Behördenverkehr: § 3 a Abs. 2 VwVfG

  [1]Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. [2]In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. [3]Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

- Identifizierung möglich?
  - Wann ermöglicht ein Pseudonym „die Identifizierung der Person“?
  - nicht nur bei Signaturen: wenn es aufgedeckt werden kann (und darf)
  - Aufdeckung nach § 14 Abs. 2 SigG ist Behörden nicht möglich, nur Polizei etc.

Datenschutz und Signaturverfahren

- „Wo kämen wir denn da hin!“
  - gemeint ist etwas ganz anderes: Behörden dürfen, Bürger nicht — genau wie beim Finanzamt, s. o.
  - Gesetzesbegründung: „Stadt München, Dezernat Jugend“ soll zulässig sein,
    „eine etwaige missbräuchliche Inanspruchnahme der Verwaltung durch eine Pseudonymverwendung, die keine Identifizierung ermöglicht“, nicht
  - Welche Gefahr hier gebannt werden soll, ist unklar — bereits jetzt kann „Dagobert Duck“ keine Sozialhilfe erhalten
  - auch ist die Versagung der Formqualität kein Schutz vor einer „missbräuchlichen Inanspruchnahme der Verwaltung“

Datenschutz und Signaturverfahren

- Seitenhieb: Wieso braucht die Verwaltung Pseudonyme?
- Und der Datenschutz?
  - Datenverwendung als Eingriff, der geringstmöglich sein muss
  - *keine* Datenerhebung, -verwendung usw. als Ziel
  - ewige Frage: Ist das Datum immer erforderlich?
    Gibt es Verfahren, die es nicht brauchen?
  - das Risiko: eine Sammlung von Zertifikaten, Signaturen, Personendaten
  - „elektronischer Rechtsverkehr“ und „elektronische Akte“
  - Durchsuchbarkeit nach Name oder Zertifikatsnummer, und zwar für sehr, sehr lange Zeiträume

Datenschutz und Signaturverfahren

- Zertifikatsnummer als „Personenkennzeichen“?
  - „eine Zahl, sie alle zu finden ...“
  - daher: kein Personenkennzeichen wie im DDR-Ausweis
  - die Ausweisnummer aus Personalausweis oder Paß darf (auch von Privaten!) nicht als Index gebraucht, und nur zur Datenpflege verwendet werden, §§ 3, 4 PAuswG, § 16 PaßG
  - für Zertifikatsnummern fehlen solche Vorschriften — kommt auf diesem Weg das „Personenkennzeichen“?
- entscheidend: keine Verknüpfung von Datenbeständen über Informationsgrenzen hinweg („informationelle Gewaltenteilung“), die Form (Nummer, Index, ...) ist zweitrangig