Betrugsprävention und Detektion aus Datenschutzsicht

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz
Schleswig-Holstein

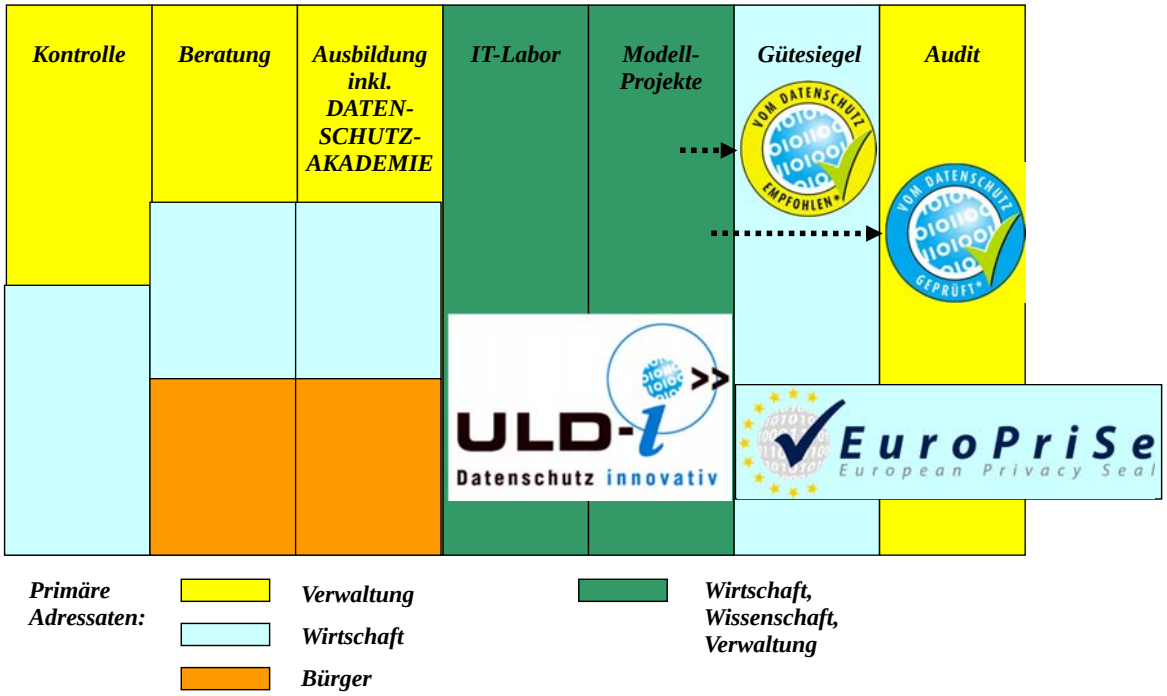
2. DIIR-Anti-Fraud-Management-Tagung

Fulda, 10.03.2011

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Rechtliche Grundlagen
- Rasterfahndung/Scoring
- Spezifische rechtliche Grenzen
- Arbeitnehmerkontrolle
- Besondere Instrumente
- Vorschläge und Ratschläge

Unabhängiges Landeszentrum für Datenschutz



Beispiele

- Schufa (ursprünglich Kreditwirtschaft)
- Wirtschaftsauskunfteien (Bürgel, Creditreform, InfoScore …)
- Hinweis- und Informationssystem (HIS – Uniwagnis) der Versicherungswirtschaft
- Black-White-List-Verfahren beim Elektronischen Lastschriftverfahren (ELV)
- Betrugsdetektion bei Kreditkartennutzung
- Fraud Prevention Tools im Einzelhandel und bei anderen Arbeitgebern
- Compliancekontrollen im Betrieb
- Internetauskunftsdienste - Personensuchmaschinen

Verfassungsrecht

- Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG
  - BVerfG 1969: Verbot von teilweise und vollständigen Persönlichkeitsbildern
  - BVerfG 1983: Grundrecht auf informationelle Selbstbestimmung = Recht selbst zu bestimmen, wer was wann bei welcher Gelegenheit über einen weiß
  - BVerfG 2008: Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme
- Art. 8 EMRK: Achtung des Privatlebens (Privat- u. Familienleben, Wohnung, Briefverkehr)
- Art. 8, 9 Europ. GrundrechteCharta: Schutz personenbezogener Daten und Privatsphäre

DIIR Deutsches Institut für Interne Revision e.V.
ULD

Volkszählungsurteil - BVerfG - 1983

- „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom **allgemeinen Persönlichkeitsrecht** … umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

- „Einschränkungen dieses **Rechts auf ´informationelle Selbstbestimmung`** sind nur im überwiegenden Allgemeininteresse zulässig.“

Schweigepflichtentbindung - BVerfG - 2003

- „Das allgemeine Persönlichkeitsrecht … entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt **auch im Privatrecht**."
- „Ist ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den **Vertragsinhalt faktisch einseitig bestimmen** kann, ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt."

DIIR Deutsches Institut für Interne Revision e.V.
ULD

7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Bundesdatenschutzgesetz – BDSG I

- § 3 IX besondere Datenkategorien
- § 3a Datenvermeidung und Datensparsamkeit
- § 4 II, III Direkterhebung beim Betroffenen, Informationspfl.
- § 4a Einwilligung
- § 6a Verbot automatisierter Einzelentscheidung
- § 6b Videoüberwachung im öffentlichen Raum
- § 9 Technisch-organisatorische Maßnahmen
- § 10 Automatisierte Abrufverfahren (Online-Abfragen)
- § 11 Datenverarbeitung im Auftrag
- § 28 Verarbeitung für eigene Geschäftszwecke
- § 28a Übermittlung an Auskunfteien

DIIR Deutsches Institut für Interne Revision e.V.
ULD

Bundesdatenschutzgesetz – BDSG II

- § 28b Scoring
- § 29 Verarbeitung zum Zweck der Übermittlung
- § 32 Verarbeitung f. Zwecke des Beschäftigungsverhältnisses
  Künftig §§ 32-32i, inbes. § 32d III
- § 33 Benachrichtigung des Betroffenen
- § 34 Auskunftsanspruch
- § 35 Berichtigung, Löschung und Sperrung
- § 38 Datenschutzkontrolle
- § 38a Verhaltensregeln
- § 42a Breach Notification
- §§ 43, 44 Bußgeld- und Strafvorschriften

Sonstige Gesetze

- Allgemeines Gleichbehandlungsgesetz (AGG)
  - § 1 AGG: Ziel des Gesetzes ist, Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen.
- Rechtsstaatsgrundsatz (Art. 19 IV GG) Diskriminierungsverbot AGB-Recht (§§ 305 ff. BGB), VerbraucherR, VertragsR
- Strafprozessual: Unschuldsvermutung, Nemo Tenetur-Grundsatz
- Betriebsverfassungsgesetz: Mitbestimmungspflicht

DIIR Deutsches Institut für Interne Revision e.V.
ULD

Das Internet als Datenquelle

- Internet als allgemeinzugängliche Quelle (§ 28 I 1 Nr. 3)
  - (Personen-) Suchmaschinen, Bewertungsportale, Google Street View, Internet-Warndienste und –auskunfteien, kriminalgeografische Apps
    - Datenbasis ist regelmäßig nicht validiert und anonym, Legalität ist nicht gewährleistet
    - Erhebung unproblematisch, Nutzung hängt von Güterabwägung ab
    - Transparenzpflicht bei Nutzung, evtl. Mitbestimmungspflicht

Auskunfteien

- Datenanlieferung nach § 28, 28a (Einwilligung, berechtigtes Interesse, kein schutzwürdiges Interesse, Beschränkung von Bonitätsbewertungen)
- Auskunftserteilung nur nach Glaubhaftmachung eines berechtigten Interesses im Einzelfall (§ 29 II)
- Benachrichtigung bei erstmaliger Übermittlung (§ 33)
- Stichprobenkontrolle (§ 10 IV 3)
- Auskunftserteilung wenn kein ü.w. Geschäftsgeheimnis (§ 34 I)

Scoring (§§ 6a, 28b, 34 II BDSG)

- Wahrscheinlichkeit künftigen Verhaltens
- Durchführung eines Vertragsverhältnisses
- Wahrscheinlichkeitswert-Berechnung nach wissenschaftlich anerkanntem mathematisch-statistischen Verfahren
- (Plausibilität der Merkmalsrelevanz)
- Datenbasis muss zulässig sein
- Grds. Verbot automatisierter Einzelentscheidung
- Berücksichtigung besonderer Verbote (Rechtewahrnehmung, AGG, z.B. ethnische Herkunft, Adresse nicht allein)
- Anspruch auf Verfahrenstransparenz
- Anspruch auf Auskunft

Rasterfahndung

- **Historischer Ursprung**: 70er Jahre Horst Herold (BKA)
  - 2002: **Suche nach Schläfern**: männlich, Student, 18-40, Moslem, arabische Herkunft
    - Datenabgleiche bei Hochschulen, Meldebehörden, Ausländerzentralregister (AZR)
    - Feinabgleiche mit Fluglizenzen, AtomG-Zuverlässigkeit, Arbeitgeber
- **BVerfG** (U.v. 4.4.2006, 1 BvR 518/02)
  - Abwägung
    - hohes Schutzziel: Bestand Bund, Länder, Leib, Leben, Freiheit
    - und hoher Eingriff: verdachtloser Eingriff, sensible Daten, Diskriminierungs- und Stigmatisierungsgefahr, große Streubreite, Einschüchterungseffekte

> Gesetz noch verfassungskonform (verlangt konkrete Gefahr)

> Maßnahme verfassungswidrig (keine konkrete Gefahr)

Präventionsdilemmata

- Umfang der erfassten Daten und der Zahl der Erfassten
  - ermöglicht die Aussagekraft von Risikoprognosen
  - verringert die Betroffenentransparenz und erhöht das Diskriminierungsrisiko

> Transparenz und unabhängige Kontrolle können helfen

- Betroffenentransparenz bzw. Veröffentlichung
  - ermöglicht Rechtsschutz und informationelle Selbstbestimmung
  - ermöglicht Umgehung und Kontrollvermeidung

> Verfahrensrechtliche Absicherungen sind möglich (Anordnung od. Kontrolle durch unabhängige Stelle)

Grenze: Zweckbindung

- Nutzung von für andere Zwecke erhobenen Daten sind grds. unzulässig
- Bei harten Negativdaten kann von Zweckbindung nach Güterabwägung abgewichen werden
- Bei weichen Negativdaten erhöhen sich die Anforderungen an Abwägung, Transparenz und Darstellung

  Bei Bonitätsbewertung gilt seit 2009 § 28a (str. bei ELV)
- Positivmerkmale dürfen nur auf Einwilligungsbasis genutzt werden

Grenze: besondere Datenkategorien

- § 3 IX: „Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.“

> Besondere Hinweispflicht bei Einwilligung: § 4a III

> Keine einwilligungsfreie Verarbeitung in Auskunfteien nach § 29 (§ 28 VI-IX)

Besonderheiten Auftragsdatenverarbeitung

- Rechtsgrundlage: § 11
  - Keine Vermischung von Daten unterschiedlicher Auftraggeber (AG) beim Auftragnehmer (AN)
  - Nutzung nur von legal durch AG erlangten Daten
  - Keine freien Auswertungsfestlegungen durch den AN
  - Keine Betriebs- und Geschäftsgeheimnisse des AN gegenüber AG (Pflicht zur vollständigen Rechenschaftslegung)
  - Beachtung der Vorgaben und Weisungen des AG
  - Festlegung technisch-organisatorischer Sicherungen im Vertrag (§ 11 II)

Arbeitnehmer-Screening I

§ 32d III BDSG-E (BR-Drs. 535/10)

- „Der Arbeitgeber darf zur Aufdeckung von Straftaten oder anderen **schwerwiegenden Pflichtverletzungen** durch Beschäftigte im Beschäftigungsverhältnis, insbesondere zur Aufdeckung von Straftaten nach den §§ 266, 299, 331 bis 334 des Strafgesetzbuchs, einen automatisierten **Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form** mit von ihm geführten Dateien durchführen. Ergibt sich ein **Verdachtsfall**, dürfen die Daten personalisiert werden. Der Arbeitgeber hat die näheren Umstände, die ihn zu einem Abgleich nach Satz 1 veranlassen, zu **dokumentieren**. Die Beschäftigten sind über Inhalt, Umfang und Zweck des automatisierten Abgleichs zu **unterrichten**, sobald der Zweck die Unterrichtung nicht mehr gefährdet wird.“

Arbeitnehmer-Screening II

Anforderungen an ein

datenschutzkonformes Screening

- Beachtung der Mitbestimmungspflicht
- Fragestellung muss vorher festgelegt werden und auf einem realen Missbrauchsverdacht basieren
- Datengrundlage muss rechtmäßig erhoben sein und für die Fragestellung plausibel relevant sein
- Beschränkung der Betroffenen auf die Risikogruppe
- Verdachtseingrenzung wird erst anonym/aggregiert vorgenommen, evtl. kollektive Mitarbeitergespräche
- Pseudonyme Erfassung mit Identifizierung nur als letztes Mittel und bei konkretisiertem Verdacht
- Kontrolle durch eine unabhängige Instanz

Fraud Prevention im Internet

- Korrekte Identifizierung des Betroffenen (künftig nPA, sowohl als Auskunftsobjekt wie bei Betroffenenansprüchen)
- Korrekte Identifizierung des Anfragenden und des berechtigten Interesses
- Rückgriff auf validierte Daten (nicht erstellt auf anonymer Basis im Internet)
- Sicherstellung der Auskunfts- und sonstige Betroffenenrechte, insbes. Widerspruchsrecht (§ 35 V)

Einschaltung Staatsanwaltschaft

- Nötig: Anfangsverdacht
- Durchführung in völliger Hoheit der StA
- Keine Usurpation staatsanwaltlicher Ermittlungsbefugnisse möglich
- Information nur über Ausgang des Verfahrens sowie, soweit dies zur StA-Ermittlung erforderlich ist
- Bereitstellung von „Fahndungsdaten“ durch StA (z.B. KUNO)

Instrument Whistle-Blowing

- Schutz der Anonymität des Informanten durch arbeitsrechtliche Garantien und Bearbeitung durch vertrauenswürdige unabhängige kompetente Stelle
- Verifikation von Anschuldigungen durch Anhörung der Betroffenen
- Abschottung der Whistleblowing-Stelle von Auftraggebern

Organisatorische Anforderungen

- Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB), unabhängig von IT, Personalabteilung, möglichst auch Sicherheit/Compliance
- Schriftliche Festlegung der Complianceverfahren unter Einschaltung des Betriebsrates und Veröffentlichung
- Anhörung des bDSB bei konkreten Maßnahmen
- Kontrolle des Ablaufs und des Abschlusses durch bDSB
- Regelmäßige Berichterstattung des bDSB gegenüber Leitung (und Betriebsrat, evtl. Belegschaft)

Branchen-Verhaltensregeln

§ 38a BDSG

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

- Bei Genehmigung durch Datenschutzaufsicht kein Kartellproblem

Schlussfolgerungen

- Compliance und Datenschutz sind mit einander vereinbar
- Kunden/Mitarbeiter/Vertragspartner sind nicht per se verdächtig
- Fraud Prevention-Verfahren können das Vertrauen in Unternehmen beeinträchtigen
- Datenschutzkonformität ist selbst eine Compliance-Anforderung

Betrugsprävention und Detektion aus Datenschutzsicht

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de