

Berichte und Thesen aus den Infobörsen

Sommerakademie 2013
„Big Data –
Informationelle Fremd- oder Selbstbestimmung?!“



www.datenschutzzentrum.de

Infobörse 1

Open Data und Big Data

- Exklusives Wissen über menschliche Verhaltensweisen
– bedarf einer Regulation
- Transparenz jedes Verfahrens – Problem: Betriebs- und Geschäftsgeheimnisse
- Eine reine „Einwilligungslösung“ ist nicht möglich
- Genehmigungsvorbehalt
- Absolute Anonymität erforderlich

Big Data in der Medizin

- Datenschutzrechtliche Grundsätze gelten für Big-Data-Analysen
- Begriff des personenbezogenen Verfahrens für unstrukturierte Datenmengen
- Lösungsmöglichkeiten
 - Privacy Impact Assessments (Datenschutzfolgenabschätzung)
 - Anonymisierung von personenbezogenen Daten
 - Aggregation
 - Kontrollfähigkeit der Verfahren
 - Transparenz der Verfahren

Outsourcing und Tracking in einer vernetzten Welt

- **Selbstzertifizierungen von US-Unternehmen** auf Basis des Safe-Harbor-Abkommens haben zur Gewährleistung des europäischen Datenschutzstandards kaum beigetragen und können nicht mehr pauschal als Legitimation für Datenübermittlungen in die Vereinigten Staaten anerkannt werden.
- Bei der **Verwendung von Standardvertragsklauseln** muss der Datenexporteur die **Aussetzung von Datenübermittlungen und gegebenenfalls einen Vertragsrücktritt** in Erwägung ziehen, wenn der Datenimporteur eine unbefugte Datenweitergabe an staatliche Stellen vornimmt.
- Beim Outsourcing personenbezogener Daten ist im Rahmen der **technisch-organisatorischen Sicherheitsanforderungen** vor allem eine Verschlüsselung nach dem Stand der Technik, eine ordnungsgemäße Protokollierung und die Gewährleistung von Mandantenfähigkeit von Bedeutung.

Scoring in Deutschland

- Die Regulierung von Scoringberechnungen nach § 28b BDSG hat grundsätzliche Defizite nicht beseitigt. Vor allem hat eine **Ausweitung der Einsatzbereiche** und eine **Erschließung neuer Datenquellen** stattgefunden.
- Berechnungen erfolgen teilweise auf der Grundlage **fehlerhafter Datenbestände**. Es werden unerhebliche Daten für bestimmtes Verhalten und diskriminierende Daten verwendet.
- Die **Aussagekraft der Berechnungsergebnisse** aufgrund der zum Einsatz kommenden Berechnungsverfahren ist fragwürdig.
- Bezüglich der Berechnungsergebnisse und -verfahren besteht für die Aufsichtsbehörden, die Betroffenen und die Auskunftsberechtigten **weiterhin hohe Intransparenz**.
- Zulässige **Einsatzbereiche** und die **zulässige Datenbasis** bestimmter Scoringverfahren, insbesondere solcher, die im Rahmen existenzieller Entscheidungen eingesetzt werden, sollten gesetzlich geregelt werden.

Social Customer Relationship Management und Datenschutz

- SCRM erweitert Möglichkeiten des Kundenbeziehungsmanagements durch Nutzung von Social Media als Datenquelle und Interaktionsplattform.
- Datenschutzrechtliche Risiken/Anforderungen bei der Ausgestaltung:
 - Unterschiedliche Erwartungen der Nutzer und der Unternehmen an die Nutzung und die Interaktion im Rahmen von Social Media
 - Intransparenz der Datenverarbeitungsvorgänge zusätzlich erhöht, Wahrnehmung Betroffenenrechte erschwert
 - Grundsätze der Datensparsamkeit und Erforderlichkeit sind in SCRM zu berücksichtigen.
- Das Projekt Sphere zielt auf eine Verbesserung der Transparenz von SCRM-Maßnahmen und -Tools innerhalb von Unternehmen ab. Es werden Unterstützungsfunktionen für die Planung, Durchführung und Kontrolle datenschutzkonformer SCRM-Initiativen entwickelt.

@rtus-Auswertung: PIAV & Co. – Big Data für die Polizei?

- Auswertungssysteme der Polizei
 - Schleswig-Holstein: @rtus-Auswertung
 - In Planung für Bund/Länder: PIAV

 - Relevanz der Daten
 - Struktur der Daten
 - Personenbezogene/anonymisierte Auswertung
- Kann die Einhaltung der Grundprinzipien des Datenschutzes bei neuer Form polizeilicher Informationsverbünde gewährleistet werden?
 - Zweckbindung
 - Erforderlichkeit

Datenschutz- und IT-Sicherheitsmanagement als Grundlage für Big Data

- Big Data wird nur zum Erfolg, wenn die rechtliche Zulässigkeit des Verfahrens gegeben ist.
- Eine umfassende Planung ist Voraussetzung für die Einführung und den Betrieb von Big-Data-Verfahren.
- Ohne Informationssicherheitsmanagementsystem (ISMS) kein ausreichender Schutz der Daten.
- Ein angemessenes Sicherheitsniveau ist in erster Linie abhängig vom systematischen Vorgehen.
- Die Unternehmensgröße und die Komplexität der Datenverarbeitung bestimmen die Parameter für die Ausgestaltung des ISMS.

Datamining-Systeme und Big Data: alles böse oder bestehen Möglichkeiten zur Zertifizierung?

- Datenschutzrecht ist in der Regel auf Datenverarbeitung im Rahmen von Big Data anwendbar, da mindestens pseudonyme Daten vorliegen.
- Im Bereich Web-Targeting und Betrugserkennung gab es schon Zertifizierungsverfahren, die zeigen, dass solche Dienste datenschutzkonform betreibbar sind.
- Gütesiegel (und Audit) sind sinnvolle Instrumente, um die Einhaltung von Datenschutz und Datensicherheit nachzuweisen und hierdurch Vertrauen zu bilden.

Privacy by Design für Big Data

- „Privacy by Design“ bezeichnet Prinzipien, deren konkrete Umsetzung eine genaue Analyse, (technische) Expertise und ein Ausbalancieren von Sicherheits- und Datenschutzinteressen erfordert
- Methoden für Big Data: De-Identifikation, Aggregation und Verschlüsselung
- [Vorstellung vor Anonymisierungstechniken und Anonymisierungsmetriken („wie anonym?“)]
- [Praktisches Problem: Semantikenkenntnisse erforderlich (z. B. bei Krankheiten), damit Anonymisierung erfolgreich]
- Testangriffe auf Anonymisierungsverfahren erforderlich (wie bei Verschlüsselungsverfahren)

Standard-Datenschutzmodell (SDM)

- Modell im Datenschutz: *Die Organisation ist der Angreifer!*
- Datenschutzspezifische *Datenschutz-Schutzziele* als Soll
- Personenbezogenes Verfahren: *Daten, Systeme, Prozesse*

- Big Data ist für alle erschwinglich (Hadoop, Neo4j, ...)
- Big Data ermöglicht Einblicke in die Komplexität von Gesellschaft *und* in das Verhalten des Individuums
- „Automatisierte Einzelentscheide“ werden zum Normalfall
- Häufig: Verwechslung von Korrelationen mit Kausalitäten
- Forderung: Beschränkung von Daten, Zwecken, Methoden
- Forderung: Genehmigungsvorbehalt