BAKER & MCKENZIE

Big Data & automatisierte Entscheidungsprozesse

RA Dr. Lukas Feiler, SSCP, CIPP/E

ARS Jahrestagung IT-Compliance
9. Juni 2015

TOPICS

I. Big Data – Realität und Mythos

II. Zunehmende Anwendbarkeit des Datenschutzrechts

III. Big Data im Konflikt mit Grundsätzen des Datenschutzrechts – Zweckbindung & Transparenz

IV. Rechtliche Anforderungen an Big Data Security

V. Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen

Big Data – Realität und Mythos – 1/2

- Big Data ist gekennzeichnet durch:
  - Volume (Menge der Daten)
  - Velocity (Geschwindigkeit der Datengenerierung)
  - Variety (Mannigfaltigkeit der Arten und Quellen der Daten)
- Datenquellen
  - Bestehende ERP-Systeme (CRM, SCM, Accounting, …)
  - Betriebliche Korrespondenz & Protokolldaten aller Art
  - Social Media
  - RFID-Scans, Geo-Location Daten
  - Machine-to-Machine (M2M) Communication (Internet of Things)
  - Audio- und Videomaterial

Big Data – Realität und Mythos – 2/2

- Anwendungsgebiete von Big Data
  - Analyse und „Vorhersage“ des Kundenverhaltens
    - Personenbezogene Werbung
    - Preisdiskriminierung
  - Optimierung betrieblicher Prozesse
    - zB Planung des Personalbedarfs
  - Risiko- und Finanzmanagement
- Mythen
  - Totale Vorhersagbarkeit (Ende des Zufalls)
  - Totale Automatisierung
  - Totale Überwachung

Zunehmende Anwendbarkeit des Datenschutzrechts

- „Datenschutzrecht betrifft uns nicht, da alle Daten ohnedies anonymisiert sind“
- Tücken der Anonymisierung
  - Wenn Personenbezug hergestellt werden kann, gilt das DSG!
  - Echte Anonymisierung ist schwierig
  - Auch M2M-Kommunikation ist häufig de-anonymisierbar!

Big Data vs. Datenschutz
Neue Ansätze zur Datenhaltung

- Altes Modell: Daten löschen, sobald nicht mehr benötigt
  - Um Speicherplatz zu sparen und Sicherheitsrisiken zu eliminieren
  - Nicht verwendete Daten als „Datenballast“
- Neues Modell: Daten aufheben
  - Zusätzlicher Speicherplatz kostet praktisch nichts mehr
  - uU finden sich neue Verwendungsmöglichkeiten für die Daten
  - Nicht verwendete Daten als „Datenschatz“

Big Data vs. Grundsätze des Datenschutzrechts

- Zweckbindung gem § 6 DSG 2000
  - Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt werden & dürfen nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden
- Datensparsamkeit gem § 6 DSG 2000
  - Verwendung von personenbezogenen Daten nur zulässig, soweit für den festgelegten Zweck wesentlich
  - → Mit Big Data zu hebender „Datenschatz“ hätte gem DSG häufig längst gelöscht werden müssen!
- Transparenz gem § 24 DSG 2000
  - Betroffene sind „aus Anlass der Ermittlung“ über Verarbeitungszwecke zu informieren

Big Data vs. Grundsätze des Datenschutzrechts – Lösungsansätze

- Volle Transparenz
- Zustimmung der Betroffenen meist erforderlich
  - Wieviel Prozent der Betroffenen werden Zustimmung erteilen?
  - Wieviel Prozent sind für Profitabilität des Big Data-Systems erforderlich?
- Vorausschauende Definition der Verarbeitungszwecke
  - Falsch: für welchen Zweck muss ich die Daten jetzt verwenden?
  - Richtig: für welche Zwecke werde ich die Daten in 3 Jahren verwenden wollen?

    → Berücksichtigung bei der Formulierung von Zustimmungserklärungen und bei Meldungen an die DSB

Rechtliche Anforderungen an die Sicherheit von Big Data

- § 14 DSG 2000: Risiko-adäquate Sicherheitsmaßnahmen
  - Risiko ist insb. von den konkreten Datenkategorien abhängig
    - Die Risiko-trächtigste Datenkategorie gibt Minimal-Anforderungen vor
  - Big Data bringt besondere Probleme
    - Putting all eggs into one basket
    - Big Data erzeugt neue Informationsflüsse - „Least privilege“ noch umsetzbar?
    - Big Data schafft neue Auswertungsmöglichkeiten (=Risiken)

→ Big Data erfordert ein zusätzliches Maß an Sicherheit

Rechtliche Anforderungen an die Sicherheit von Big Data / Access Control

- Zugriffsberechtigungen müssen Datenverwendung durch Unbefugte verhindern (§ 14 Abs 2 Z 5 DSG 2000)
  - Nicht jeder Mitarbeiter wird befugt sein, alle Daten für alle Zwecke zu verwenden (zB Gesundheitsdaten der Mitarbeiter)
  - Logical Access Control muss die Verwendung bestimmter Datenkategorien auf bestimmte Nutzer/Rollen beschränken
  - Daten sind jedoch oft unstrukturiert & dynamisch

→ Manuelle Rechtevergabe nicht möglich

→ Big Data-basiertes Access Management?

Compliance-Risiken durch automatisierte Entscheidungen – 1/4

- Bei vollautomatischen Entscheidungen ohne menschlichen Plausibilitäts-Check:
  - Besonders hohe Anforderungen an
    - Qualität und Vollständigkeit der Daten
    - Datenintegrität (§ 6 Abs 1 Z 3 DSG 2000)
  - Was sind die Datenquellen?
  - Welchen Sicherheitsanforderungen unterlagen die Datenquellen?
  - → Wenn Datenquellen für automatisierte Entscheidung nicht geeignet:
    - Datenschutz-Verletzung
    - Zivilrechtliche Haftung gegenüber Vertragspartnern bei fahrlässig automatisierten Entscheidungen?

Compliance-Risiken durch automatisierte Entscheidungen – 2/4

- Vollautomatisierte Entscheidungen unzulässig, wenn (§ 49 DSG 2000):
  - rechtliche Folgen od. erhebliche Beeinträchtigung für Betroffenen &
  - Entscheidung auf Grundlage der Bewertung einzelner Persönlichkeitsaspekte des Betroffenen (zB Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit)
  - Ausnahmen:
    - Wahrung berechtigter Interessen des Betroffenen garantiert (zB durch Möglichkeit, seinen Standpunkt geltend zu machen) oder positive Entscheidung über Ersuchen des Betroffenen hinsichtlich Abschluss/Erfüllung eines Vertrages
    - Falls ausnahmsweise zulässig: logischer Ablauf der Entscheidungsfindung ist allgemein verständlich darzulegen

Compliance-Risiken durch automatisierte Entscheidungen – 3/4

- Vollautomatisierung daher grds unzulässig bei
  - Entscheidung über die Nicht-Gewährung von Mitarbeiterboni auf Grundlage der errechneten Leistungsfähigkeit
  - Kreditverweigerung wegen errechneter Unzuverlässigkeit
  - Endgültige vollautomatisierte Entscheidung über Art des Implantats auf Grundlage der errechneten Lebenserwartung & „Lebensfreude“
- Vollautomatisierung daher zulässig bei
  - Entscheidung über die Gewährung von Rabatten auf Grundlage der Finanzstärke der Kunden
  - Entscheidung über die Zusendung personenbezogener Werbung

Compliance-Risiken durch automatisierte Entscheidungen – 4/4

- Lösungsansätze für die Praxis:
  - Compliance Risk Assessment
  - Segmentierung von Entscheidungsprozessen und De-Automatisierung der kritischen Entscheidungen
  - Menschliche Kontrolle durch Daten-Analysten:
    - Kontrolle der Entscheidungsgrundlage
    - Stichprobenartige Kontrolle der automatisierten Entscheidungen

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com