BAKER & MCKENZIE

Rechtliche Risiken von Big Data und automatisierten Entscheidungen

RA Dr. Lukas Feiler, SSCP, CIPP/E

Fraud Tagung 2016
10. März 2016

Big Data – Realität und Mythos

- Big Data ist gekennzeichnet durch:
  - Die automatisierte Analyse von idR unstrukturierten großen Datenmengen
- Datenquellen
  - Bestehende ERP-Systeme (CRM, SCM, Billing, …)
  - Betriebliche Korrespondenz & Protokolldaten aller Art
  - Social Media, RFID-Scans, Geo-Location & M2M-Daten, …
- Anwendungsgebiete von Big Data
  - Analyse und „Vorhersage“ des Kundenverhaltens
  - Optimierung betrieblicher Prozesse - zB Planung des Personalbedarfs
  - Risiko- und Finanzmanagement

Fortschreitende 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 (zB anonymisierte Netflix-Bewertungen, Standortdaten)
  - Auch M2M-Kommunikation ist häufig de-anonymisierbar!

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

Herausforderungen durch sich wandelnde Verarbeitungszwecke – 1 von 2

- 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“

Herausforderungen durch sich wandelnde Verarbeitungszwecke – 2 von 2

- Problem: Zweckbindung gem § 6 DSG 2000
  - Festgelegter, eindeutiger Verarbeitungszweck erforderlich
  - → Speicherung auf Vorrat für undefinierte Zwecke unzulässig
- Problem: Prinzip der Datensparsamkeit gem § 6 DSG 2000
  - Verwendung v. Daten nur zulässig, wenn für festgelegten Zweck wesentlich
  - → Mit Big Data zu hebender „Datenschatz“ muss häufig gem DSG gelöscht werden!
- Lösungsansatz aus Unternehmenssicht
  - → Vorausschauende Definition der Verarbeitungszwecke

Automatisierte Entscheidungen – 1 von 2

- Vollautomatisierte Entscheidungen unzulässig, wenn (§ 49 DSG 2000):
  - rechtliche Folgen od. erhebliche Beeinträchtigung für Betroffenen
  - und 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
    - E im Rahmen des Abschlusses od. Erfüllung eines Vertrages und Ersuchen des Betroffenen stattgegeben
  - Falls ausnahmsweise zulässig: logischer Ablauf der Entscheidungsfindung ist allgemein verständlich darzulegen

Automatisierte Entscheidungen – 2 von 2

- Beispiele für vollautomatisierte Entscheidungen – zulässig?
  - Endgültige vollautomatisierte Kreditverweigerung wegen errechneter Unzuverlässigkeit
  - Vollautomatisierte Entscheidung über die Gewährung von Rabatten auf Grundlage der Finanzstärke der Kunden
  - Vollautomatisierte Entscheidung über Sperrung des Internet-Zugangs wegen Weiterverbreitung von Malware und Angriff auf andere Teilnehmer

Automatisierte Entscheidungen nach DSGV

- Verbot gilt unabh., ob Persönlichkeitsaspekte als Grundlage
- Zulässig wenn (Art 20 Abs 1a DSGV)
  - für Abschluss oder Erfüllung eines Vertrages mit Betroffenen erforderlich (grds keine sensiblen Daten)
  - von nationalem Recht gedeckt
  - ausdrückliche Einwilligung der betroffenen Person
- Zusätzliche Pflichten
  - Gewährung des Rechts auf (1) „human intervention“, (2) Darlegung des eigenen Standpunkts und (3) Anfechtung der Entscheidung
  - Informationspflicht bei Datenerhebung über (1) Bestehen einer automatisierten Entscheidungs, (2) verwendete Logik und (3) Tragweite und Auswirkungen der Entscheidung

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