BAKER & MCKENZIE

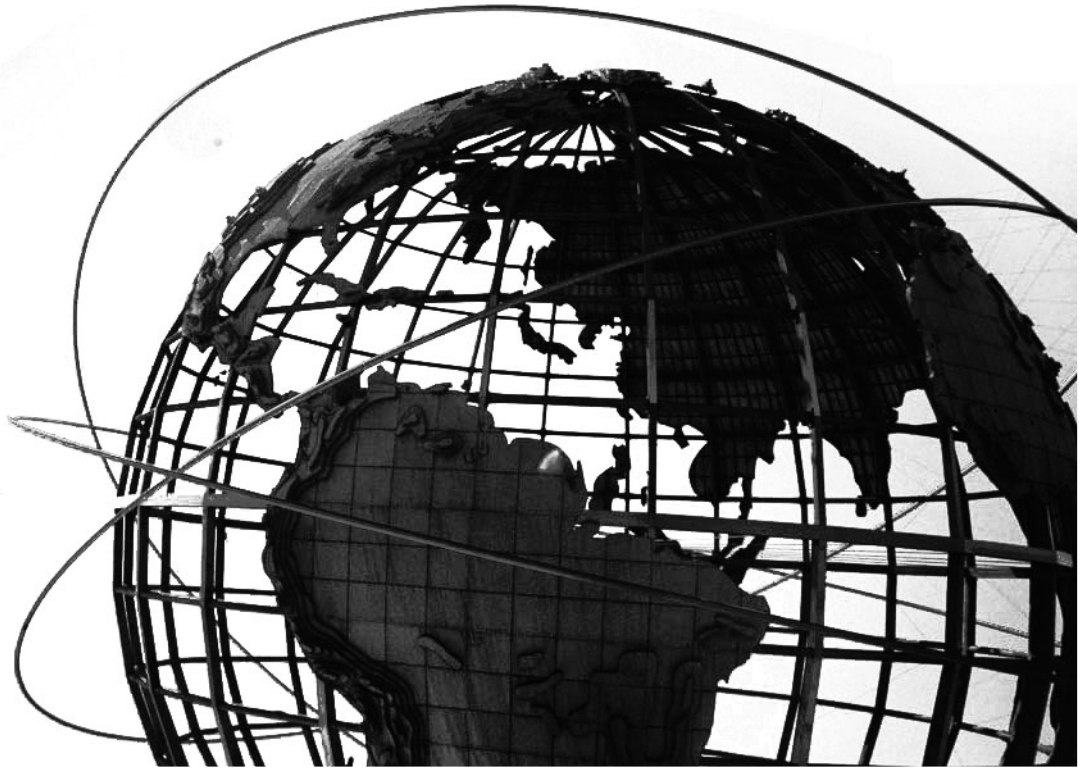
# Big Data – Big Liability?

## Rechtliche Risiken durch Big Data

Dr. Lukas Feiler, SSCP

Security Forum 2013

17. April 2013



# Themen

I. Big Data – Realität und Mythos

II. Fortschreitende Anwendbarkeit des Datenschutzrechts

III. Rechtliche Anforderungen an die Sicherheit von Big Data

IV. Herausforderungen durch sich wandelnde Verarbeitungszwecke

V. Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen

# Big Data – Realität und Mythos - 1

- Big Data ist gekennzeichnet durch:
  - Die automatisierte Analyse (Data Mining) von
  - idR unstrukturierten
  - großen Datenmengen
- Datenquellen
  - Bestehende ERP-Systeme (CRM, SCM, Accounting, …)
  - Betriebliche Korrespondenz & Protokolldaten aller Art
  - Social Media
  - Audio- und Videomaterial
  - RFID-Scans, Geo-Location Daten
  - Machine-to-Machine (M2M) Communication

©2013 Baker & McKenzie

# Big Data – Realität und Mythos - 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

©2013 Baker & McKenzie

# 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, AOL-Suchanfragen, Standortdaten)
  - Auch M2M-Kommunikation ist häufig de-anonymisierbar!

©2013 Baker & McKenzie

# 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

©2013 Baker & McKenzie

# Rechtliche Anforderungen an die Sicherheit von Big Data – Logical 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?

©2013 Baker & McKenzie

# Herausforderungen durch sich wandelnde Verarbeitungszwecke - 1

- 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“

©2013 Baker & McKenzie

# Herausforderungen durch sich wandelnde Verarbeitungszwecke - 2

- Problem: 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
  - → Speicherung auf Vorrat für undefinierte Zwecke unzulässig
  - → Jede Zweckänderung kann neue Registrierungs- und Zustimmungspflichten begründen (neue Datenanwendung)
- Problem: Prinzip der Datensparsamkeit gem § 6 DSG 2000
  - Verwendung von personenbezogenen Daten nur zulässig, soweit für den festgelegten Zweck wesentlich
  - → Mit Big Data zu hebender „Datenschatz“ muss häufig gem DSG gelöscht werden!

©2013 Baker & McKenzie

# Herausforderungen durch sich wandelnde Verarbeitungszwecke - 3

- Lösungsansatz aus Unternehmenssicht
  - 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 bei der DSK

    → Volle Transparenz

©2013 Baker & McKenzie

# Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen - 1

- Bei vollautomatischen Entscheidungen ohne menschlichen Plausibilitäts-Check:
  - Besonders hohe Anforderungen an
    - Qualität und Vollständigkeit der Daten
    - Datenintegrität
  - Was sind die Datenquellen?
  - Welchen Sicherheitsanforderungen unterlagen die Datenquellen?
  - → Wenn Datenquellen für automatisierte Entscheidung nicht geeignet:
    - Datenschutz-Verletzung
    - Zivilrechtliche Haftung gegenüber Vertragspartnern wegen Verletzung vertraglicher Nebenpflichten

©2013 Baker & McKenzie

# Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen - 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:
    - Insb. wenn Wahrung berechtigter Interessen des Betroffenen garantiert (zB durch Möglichkeit, seinen Standpunkt geltend zu machen)
    - Falls ausnahmsweise zulässig: logischer Ablauf der Entscheidungsfindung ist allgemein verständlich darzulegen

©2013 Baker & McKenzie

# Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen - 3

- Beispiele für vollautomatisierte Entscheidungen:
  - Endgültige vollautomatisierte Entscheidung über die Nicht-Gewährung von Mitarbeiterboni auf Grundlage der errechneten Leistungsfähigkeit
  - Endgültige vollautomatisierte Kreditverweigerung wegen errechneter Unzuverlässigkeit
  - Endgültige vollautomatisierte Entscheidung über Art des Implantats auf Grundlage der errechneten Lebenserwartung & „Lebensfreude“
  - Vollautomatisierte Entscheidung über die Gewährung von Rabatten auf Grundlage der Finanzstärke der Kunden
  - Vollautomatisierte Entscheidung über die Zusendung personenbezogener Werbung

©2013 Baker & McKenzie

# Rechts- und Sicherheitsrisiken durch automatisierte Entscheidungen - 4

- Lösungsansätze für die Praxis:
  - Datenschutz-Compliance
    - Erhöhte Sicherheitsanforderungen – Big Data needs Big Security
    - Keine vollautomatisierten Entscheidungen auf Grundlage von Persönlichkeitsaspekten, die rechtliche Folgen od. erhebliche Beeinträchtigung für Betroffene bringen
  - Zivilrechtliches Haftungsrisiko minimieren:
    - Big Data erfordert menschliche Kontrolle
    - Um Fehler in den Datenquellen zu erkennen, sind gute Analysten erforderlich

©2013 Baker & McKenzie

# Kontakt

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

**Dr. Lukas Feiler, SSCP**
**lukas.feiler@bakermckenzie.com**

Die Baker & McKenzie - Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern und Solicitors ist eine im Partnerschaftsregister des Amtsgerichts Frankfurt/Main unter PR-Nr. 1602 eingetragene Partnerschaftsgesellschaft nach deutschem Recht mit Sitz in Frankfurt/Main. Sie ist assoziiert mit Baker & McKenzie International, einem Verein nach Schweizer Recht. Mitglieder von Baker & McKenzie International sind die weltweiten Baker & McKenzie-Anwaltsgesellschaften. Der allgemeinen Übung von Beratungsunternehmen folgend, bezeichnen wir als "Partner" einen Freiberufler, der als Gesellschafter oder in vergleichbarer Funktion für uns oder ein Mitglied von Baker & McKenzie International tätig ist. Als "Büros" bezeichnen wir unsere Büros und die Kanzleistandorte der Mitglieder von Baker & McKenzie International.

© Baker & McKenzie