HERAUSFORDERUNG BIG DATA FÜR DIE WIRTSCHAFT

Mag. Stefan Panic

Mittwoch, 26. April 2017

Einleitung

- Begriff Big Data
  - Ein Sammelbegriff – unterschiedliche Rechts- und Problembereiche
- Big Data und Datenschutz
  - Probleme und Lösungsansätze
  - Voraussetzungen
- Nichtpersonenbezogene Big Data
  - Herausforderungen
  - Entwicklungsbedarf

Was ist "Big Data"?

- Zusammenfassung unterschiedlicher Begriffe → unterschiedliche Rechtsfolgen
  - Keine Legaldefinition
  - Kein einheitlicher Begriff
  - Hauptmerkmal Datenmenge
    - Datenmengen, die aufgrund ihrer Größe oder Komplexität mit herkömmlichen Methoden der Datenverarbeitung nicht mehr verarbeitet werden können
  - Verwendung in neuen Bereichen, die zT erst durch Big Data entstehen
  - "V" – Volume, Variety, Velocity, Variability, Veracity
  - "next level" der Datenverarbeitung

Big Data in der Rechtsordnung

- Personenbezogene Big Data
  - Einschränkung der Verarbeitung durch Beschränkungen in Datenschutzrecht
- Nichtpersonenbezogene Big Data
  - freie Verarbeitung außerhalb des Datenschutzrechts
  - Aber:
    - Daten als Rechts- und Wirtschaftsgut?
    - Ökonomische Aspekte hinsichtlich (fehlender?) Schutzfähigkeit?

Anwendungsbereiche von Big Data

- Breites Spektrum der Sektoren in welchen Big Data eine Rolle spielen könnte oder eine Chance darstellen könnte
  - IT und Technology – die "üblichen Verdächtigen" bei der Verarbeitung von Big Data (Amazon, Google, Facebook etc.)
  - "Internet of Things" und "Industrie 4.0" – diverse Anwendungen, bei welchen personen- und maschinenbezogene Daten entstehen (Smart Factories, Smart Homes, Verkehrssteuerung, "vernetzte Autos" etc.)
  - Gesundheitssektor
  - Retail – kundenbezogene Auswertungen

Big Data und Datenschutz

- Personenbezogene Big Data
  - Gesundheitssektor: weitreichende Analysen von Patientendaten
  - IT-Sektor: der "gläserne Nutzer / Kunde" – detaillierte Auswertungen von Kunden- und Nutzerdaten im Internet für auf die konkrete Person zugeschnittene Angebote
  - Sonstige personenbezogene Analysen (zB Kaufkraft)
- Datenschutzrechtliche Rahmenbedingungen
  - Grundsätzliche Schranken, die aus den Grundprinzipien folgen
  - Weitere spezifische Voraussetzungen für die Datenverarbeitung
  - Praktische Hindernisse

Datenschutzrechtliche Grundprinzipien (I)

- **Datenminimierung / Wesentlichkeitsgrundsatz**
  - Widerspricht weitgehend dem Wesen von Big Data – *per se* Einschränkung der Möglichkeiten der Datensammlung
  - Verbot von "Data Warehousing" und "Data Mining" – Datenbeschaffung und -verarbeitung "auf Vorrat"
  - Zweckbezogene Datenminimierung - Lösung durch breit angelegte Zweckbeschreibungen?
- **Zweckbindung**
  - Erschwernis der zweckübergreifenden Datenverarbeitung – Festlegung des Zwecks vor der Datensammlung
  - Zweckänderung = Datenübermittlung
  - Aufweichung durch DSGVO (Art 6 Abs 4) – Zweckänderung auf "verbundene" Zwecke zulässig?

Datenschutzrechtliche Grundprinzipien (II)

- Weitere problematische Prinzipien:
  - Richtigkeits- und Aktualitätsgrundsatz
    - Gewährleistung bei größeren Datenmengen unter Umständen schwierig
  - Datensicherheit und Datengeheimnis
    - Datensicherheit muss der Art, dem Zweck und dem Umfang der Verarbeitung entsprechen – "big security for big data"
  - Transparenz der Verarbeitung
    - Eventuell negative Beeinflussung durch die Datenmengen

Datenschutzrechtliche Grundprinzipien – Lösungsansätze (I)

- Verarbeitung aufgrund der Zustimmung der Betroffenen?
  - Informierte Zustimmung notwendig, dh Zwecke und Datenarten müssen identifiziert werden
  - Wirksamkeit – Freiwilligkeit – Geschäftsfähigkeit
  - Ist nur eine Rechtsgrundlage für die Rechtsmäßigkeit der Verarbeitung, befreit aber nicht von der Einhaltung der Grundprinzipien!
  - Meist keine Lösung sondern eine Voraussetzung (zB *Profiling*)
- Anonymisierung und Pseudonymisierung
  - Rechtlich zufriedenstellende Lösung – anonymisierte Daten unterliegen nicht der DSGVO
  - Aber: volle Anonymisierung oft technisch schwierig und dem eigentlichen Zweck widersprechend (außer bei "industriellen" Anwendungen)
  - Pseudonymisierung grundsätzlich vorausgesetzt durch die DSGVO

Datenschutzrechtliche Grundprinzipien – Lösungsansätze (II)

- Privilegierung wissenschaftlicher oder geschichtlicher Forschung und Statistik
  - Ausdrückliche Ausnahme vom Zweckbindungsprinzip (Art 5 Abs 1 lit (b) DSGVO)
  - Enger Anwendungsbereich in der Privatwirtschaft außerhalb der Forschungseinrichtungen
  - Konkrete Regelungen weitgehend offen (Art 89 Abs 2 DSGVO)

Anwendbare Regelungen – rechtliche Voraussetzungen (I)

- Eine Reihe von spezifischen Voraussetzungen zusätzlich zu den Grundprinzipien
- Schwierigkeiten bei der Feststellung der Grundlagen für die Rechtmäßigkeit bei Datenmengen von Big Data und unbestimmten Zwecken
  - Zustimmung als mögliche Grundlage; aber – Bestimmtheit
  - Überwiegende berechtigte Interessen
- Automatisierte Einzelentscheidungen und Profiling (Art 22 DSGVO)
  - Zustimmung wird oft vorausgesetzt sein!
- "Privacy by design and default" (Art 25 DSGVO)
  - Konkretisierung der Grundprinzipien, welche zur Pseudonymisierung und Datenminimierung "zwingen"

Anwendbare Regelungen – rechtliche Voraussetzungen (II)

- Folgeabschätzung (DPIA – Art 35ff DSGVO)
  - Anwendbar bei "systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling, gründet" → Anwendungsfall Big Data
- Verpflichtender Datenschutzbeauftragter?
  - Bei Verarbeitung von sensiblen Daten (zB Gesundheitssektor)
  - Ansonsten: nur wenn die Kerntätigkeit "eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen" erforderlich macht

Weitere praktische Hindernisse

- Großflächige Datenweitergaben
  - oft eine Notwendigkeit bei großen Datenmengen (Server-Platz / Speicherung in der Cloud)
  - Voraussetzungen für Datenweitergaben ins (nicht-EWR) Ausland – großes Netz von Verträgen
  - Erleichterungen durch die DSGVO im Vergleich zum DSG (formale Voraussetzungen)
- Ausgebaute Betroffenenrechte
  - praktische Schwierigkeiten bei größeren Daten- und damit Betroffenenmengen
  - Dasselbe Problem bei einem allfälligen Data Breach

Big Data außerhalb des Datenschutzrechts

- Großer praktischer Anwendungsbereich in der Industrie und Technologie
  - "Internet-of-Things"
  - Smart Homes
  - Smart Factories / Monitoring
- Daten sind weitgehend nicht personenbezogen bzw. steht der Personenbezug nicht im Fokus
  - Anonymisierung leichter durchführbar
  - Allerdings: Verarbeitungspotential von Daten in personenbezogener Form? (etwa Fahrverhalten?)
  - Weitere Erleichterung durch DSGVO – unternehmensbezogene Daten sind nicht mehr personenbezogene Daten

Daten als Rechtsgut?

- Außerhalb des Datenschutzes ergeben sich andere Fragen – insbesondere die der Schutzfähigkeit der erzeugten Daten – Daten als Rechts- und Wirtschaftsgut
- Überlegung zum "Daten-Schutz" – Daten und nicht der Betroffene im Mittelpunkt?
- Rechtsordnung sieht keine Hindernisse vor, aber auch keinen Schutz
- Kollision mit dem Datenschutz – wenn Daten doch mit Personenbezug einen Wert haben

Lösungsansätze für Schutz von Daten

- Urheberrechtlicher Schutz?
  - nur für Datenbanken, aber nicht für einzelne Datensätze
  - Eingeschränkter Schutz bei wesentlichen Entnahmen
- Betriebs- und Geschäftsgeheimnisse?
- Weiter Sachbegriff des ABGB – sachenrechtlicher Schutz?
- UWG und sonstiger deliktischer Schutz?

- Rechtspolitische Überlegung – ist der Schutz von Daten sinnvoll?
  - Notwendigkeit?
  - Grenzen des Schutzes?

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Für weitere Fragen stehen wir gerne zur Verfügung!

Mag. Stefan Panic
stefan.panic@dlapiper.com

DLA Piper Weiss-Tessbach
Rechtsanwälte GmbH
Schottenring 14
1010 Wien
Telefon: +43 (0)1 531 78 - 1034
Fax: +43 (0)1 533 52 52