Big Data Analytics
vs.
Data Protection

Norbert Nolte, 9 February 2015
Agenda

1. Legal Framework
2. Data Usage
3. Research Privileges
4. Challenges for Big Data Analytics
Legal Framework (1)

- EU Charter of Fundamental Rights of 2012

  - Minimum harmonization
  - Implementation required in each Member State

- German Federal Data Protection Act (BDSG) of 1990
  - Regulates private corporations as well as authorities
  - Complemented by sector specific regulation
    (e.g. TMG = Internet, TKG = telecoms, SGB = health care)

- 16 State Data Protection Acts in Germany
  - Regulation of authorities / public entities of the Länder
  - Hessen enacted the first data protection act already in 1970
Legal Framework (2)

- In the making: EU Data Protection Regulation
  - Maximum harmonization
  - Will replace Directive 95/46/EC and create a uniform data protection framework
  - Directly applicable in each Member State (no implementation required)
  - Enforcement remains local though
Data Usage

- What is protected: (only) personal data
  - Data must refer (directly or indirectly) to an individual (e.g. IP address)
    - any link is sufficient
  - Very protective rules for sensitive data (e.g. health related data, religion)
  - Less rigid regime for pseudonymized data (e.g. credit card data)
  - Not applicable for anonymized data (but: no clear guidance on technical requirements)

- General principle
  - Collection, processing and use prohibited unless particularly justified
    (nothing is allowed, unless it’s allowed!)
  - Even changing the purpose for the use of data requires a justification
    (e.g. using customer data for big data analytics)

- Justification
  - Written consent (outdated?), electronic consent (e.g. on the Internet)
  - Statutory justification (often: weighting of interests → legal uncertainty)
Research Privileges

- Justification without consent – even for sensitive data
  - Research must be conducted by an independent research facility
  - Data is used for research purposes only (*purpose limitation*)
  - The data subject has a right to object to the use of his/her data
  - Research data is anonymized or at least pseudonymized to the extent possible
  - De-anonymization allowed if this is required by the research purpose

- Consent orally or electronically
  - But only if written consent would materially impede the research purpose (e.g. telephone or email surveys)

- No duty to notify the data subject of data transfers
  - But only if a notification involves a disproportionate effort for the research facility
Challenges for Big Data Analytics (1)

- **Big Data = personal data?**
  - In theory, any anonymized data can be linked back to an individual (by way of combining a sufficiently large set of information)
  - There is a pending case at the European Court of Justice (ECJ) to further clarify the term personal data (in this case regarding IP addresses)

- **Principle of data minimisation**
  - Data must be deleted when not needed anymore (for the original purpose)
  - BUT: Big Data is all about storing as much data as possible and see how it can be used (afterwards)
  - For data use by governments, the ECJ has decided that data retention (*Vorratsdatenspeicherung*) is only possible if there are effective safeguards in place to prevent the misuse of data and precise guidance is available in this respect
Challenges for Big Data Analytics (2)

- Researchers must guarantee data security
  - Research facilities have to implement effective technical and organisational measures for data security (e.g. state of the art cybersecurity)
  - If research facilities grant each other or private businesses access to "their" data, they might become liable for any non-compliance of these third parties; the same is true for external service providers (dropbox, cloud services providers)

- Data transfer outside the EU/EEA
  - Possible if the recipient's country has an "adequate level of data protection" (e.g. Switzerland or New Zealand, but not the US or China) or
  - There are means to ensure the adequate level of data protection (e.g. EU Standard Contractual Clauses, Binding Corporate Rules, Safe Harbour re the US)
  - Challenges re cloud/web storage
Thank you!

Contact Information:

Prof. Dr. Norbert Nolte

Freshfields Bruckhaus Deringer LLP
Im Zollhafen 24
50678 Cologne

Email: norbert.nolte@freshfields.com
T +49 221 20 50 70
F +49 221 20 50 79 0