Introduction to the proposed European Privacy Law Reform

- The German Perspective -

Frankfurt, February 2012

Rechtsanwalt
Dr. Ulrich Wuermeling, LL.M. (London)

ulrich.wuermeling@lw.com
Overview

Part 1: Reform Package

Part 2: Consequences for Germany
PART 1
REFORM PACKAGE
Data Protection is a European issue

- European Data Protection Directive (95/46/EC)
- Article 29 Data Protection Working Party
- Recognition of adequacy of data protection (especially Switzerland, Safe Harbour in the USA)
- Recognition of Model Clauses
- Agreements regarding airline passenger records and finance data
- European Charter of Fundamental Rights (Article 8)
- Treaty on the Functioning of the European Union (“TFEU”) (Article 16, 114)
Europe is a patchwork of nations

- Different standards resulting from inconsistent implementation of Directives into national laws
- Independent national data protection supervisory authorities cause further inconsistency
- Special regulations on a national level (e.g. in Germany regarding advertising, credit reporting agencies and scoring)

European Court of Justice
Judgment of 24 November 2011 (C-468/10 and C-469/10)

“harmonization which is generally complete”
## Process leading to the reform package

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>Public consultation for the implementation of the European Data Protection Directive</td>
</tr>
<tr>
<td>2009</td>
<td>Review of the legal framework regarding data protection</td>
</tr>
<tr>
<td>2009</td>
<td>Public consultation</td>
</tr>
<tr>
<td>2010</td>
<td>Public consultation</td>
</tr>
</tbody>
</table>
| 2011 | Inter-service consultation regarding the draft reform package  
• General Data Protection Regulation  
• Data Protection Directive regarding Police Co-operation and Judicial Co-operation in criminal matters |
| 2012 | First European Commission proposal |
Process leading to the Regulation

European Commission proposal dated 25 January 2012

First Reading
Parliament and Council

Second Reading
Parliament and Council
Entry into force of the Regulation

- European Regulations are **directly** applicable
- No implementation into national law
- Provision contained in proposal (Article 91)
  - Entry into force on the twentieth day following that of its publication in the Official Journal of the European Union
  - Applicable two years from publication date

- Will national law become obsolete?

2016?
The positive aspects of the reform

European Commission Communication:

• Individuals will be put in control of their data
• Data protection rules adapted to digital internal market
  • Harmonization (EUR 2.3 billion savings through standardizing of divergent data protection rules)
  • Simplification (EUR 130 million savings through elimination of the requirement for general notification to the supervisory authority)
  • More independence for data protection supervisory authorities
  • One-Stop-Shop for data protection within the European Union
  • More efficient co-operation between data protection supervisory authorities
  • More consistent application of data protection law
• Sets global standards for data protection
Does the patchwork of nations remain?

- National data protection supervisory authorities remain independent but will be governed more strictly by the European Commission concerning the application of data protection law.
- Statutory obligations for data processing continue to be determined predominantly pursuant to national law.
- Special areas of leeway with regard to implementation provided for in the General Data Protection Regulation:
  - Rights of data subjects (Article 21) -> with exceptions
  - Press (Article 80) -> with exceptions
  - Health (Article 81) -> only stricter
  - Protection of employee data (Article 82) -> only stricter
  - Research purposes (Article 83) -> only stricter
  - Obligations of secrecy (Article 84) -> only stricter
  - Churches and religious associations (Article 85) -> only stricter
  - ePrivacy Directive (Article 89): implementation on a national level remains
Further development of data protection

- European Data Protection Board (Article 64)
  - Composition
    - representatives of supervisory authorities of each Member State
    - representative of the European Data Protection Supervisor
    - European Commission shall have the right to participate in the activities and meetings
    - NO representation of national governments
    - NO representation of the industry
  - Advisory, investigative and reporting function
  - Expression of opinions

- Rights of the European Commission
  - 26 enabling provisions for “delegated acts”
    -> right to object for European Parliament and Council (Article 86)
  - 20 powers for “implementing acts”
PART 2
CONSEQUENCES FOR GERMANY
Definition of „personal data“

- The European Data Protection Directive 1995 protects data
  - concerning identified natural persons
  - concerning identifiable natural persons
  - also in business situations (B2B)
- Controversial debate regarding “identifiable”
  - IP-Addresses
  - Cookies (also difficult in the ePrivacy Directive)
  - Online Behavio(u)ral Advertising (OBA)
- Draft General Data Protection Regulation
  (Article 4 and Recitals 23 and 24)
  - Data subject identifiable by controller or third parties “by means reasonably likely to be used”
  - Online identifiers and IP addresses need not necessarily be considered as personal data in all circumstances
# New approaches to regulation

<table>
<thead>
<tr>
<th>Article</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Extra-territorial effect</td>
</tr>
<tr>
<td>8</td>
<td>Processing of personal data of a child</td>
</tr>
<tr>
<td>17</td>
<td>Right to be forgotten and to erasure</td>
</tr>
<tr>
<td>18</td>
<td>Right to data portability</td>
</tr>
<tr>
<td>20</td>
<td>Restriction on profiling</td>
</tr>
<tr>
<td>23</td>
<td>Data protection by design and by default</td>
</tr>
<tr>
<td>24</td>
<td>Joint controllers</td>
</tr>
<tr>
<td>13, 26, 28, 29, 30, 33, 42, 44, 51, 77</td>
<td>Responsibilities and obligations of the processor</td>
</tr>
<tr>
<td>31, 32</td>
<td>Data breach notification</td>
</tr>
<tr>
<td>46-72</td>
<td>Supervision and new role of the European Commission</td>
</tr>
<tr>
<td>73-79</td>
<td>Remedies, Liability and Sanctions</td>
</tr>
</tbody>
</table>

---
Restrictions for the use of personal data

  - No obligation to strictly specify purposes
  - Collection and use of data also for third party interests

- Draft General Data Protection Regulation
  (Article 6 para. 1 (f) and para. 4)
  - Balance of interest clause no longer allows the taking into account of third party interests (so far permitted by Section 29 para. 2 BDSG)
  - Obligation to strictly specify purposes cannot be overcome by balance of interest clause
  - A ban on commercial direct marketing without a declaration of consent has been deleted from earlier drafts. Instead, there is a right to object and obligation to inform
  - Restrictions for individuals under 18 years of age
Requirements for a valid declaration of consent

  - Informed consent
  - No coercion
- Additional requirements in Germany
  - Must be in writing (= signature)
  - Highlighted
  - Limitations of general terms and conditions
- Draft General Data Protection Regulation (Article 7 and Recitals 25, 32)
  - Burden of proof is provided for
  - Explicit (“by ticking a box”)
  - Imbalance of power is not allowed
  - Withdrawal of consent is always possible
Extended obligation of transparency

  - Identity of controller and obligation to specify purposes
  - If “necessary” also
    - categories of recipients
    - obligation to reply and consequences of refusal
    - existing rights of access and rectification
- Draft General Data Protection Regulation
  (Article 14 and 15 and Recitals 46, 48 and 51)
  - Retention period
  - Right of access, rectification or erasure
  - Right to lodge a complaint with a supervisory authority and their contact data
  - Intended data transfers to third countries
  - Obligation to make available data and consequences of refusal
  - Source from which the data originate
Right to be forgotten

  - Deletion of data unlawfully retained
  - Right to object in case of overriding interest
  - Right to object against direct marketing
- Draft General Data Protection Regulation (Article 17 and Recital 53)
  - Deletion if
    - objection has been lodged and if there are no convincing and overriding reasons to the contrary (change in the burden of proof)
    - withdrawal of consent
  - Deletion from publicly accessible sources
  - Exceptions (especially statutory storage requirements)
Right to data portability

- General right of access and erasure in the European Data Protection Directive 1995
- Similar in the German Data Protection Act (Bundesdatenschutzgesetz)
- Draft General Data Protection Regulation (Article 18 and Recital 55)
  - right to obtain a copy of the data in an electronic and structured format which is commonly used
  - right of the data subject to disclose personal data to third parties
  - the European Commission may specify the electronic formats
Measures based on profiling

• Provision regarding “automated individual decisions” in the European Data Protection Directive 1995
  • Legal or material adverse effects
  • Based solely on automated processing of data
• Data Protection Amendments 2009 introduced additional special scheme regarding scoring
• No application to scoring for advertising purposes
• Draft General Data Protection Regulation (Article 20)
  • Solely automated processing
  • Produces legal effects for or significantly affects the individual
  • Evaluation, analysis or prediction
  • Limited number of exceptions only, therefore a declaration of consent will be necessary in many cases
The role and responsibility of service providers

- European Data Protection Directive (Article 2 f and 17 para. 3)
  - Processor is not third party
  - Only on instruction from the controller
  - Technical and organizational measures
- Extension through Data Protection Amendments 2009
  - 10-point catalogue for the drawing up of contracts
  - Security audits must be recorded
- General Data Protection Regulation (Articles 13, 26, 28, 29, 30, 33, 42, 44, 51 and 77 and Recitals 62, 65 and 66)
  - Requirements for contractual regulations
  - More responsibilities for processor
Limitations for third country data transfers

  - Only export to countries with “adequate protection” – white list
  - Approved methods of adequacy:
    - Safe Harbo(u)r
    - Model Clauses
    - Binding Corporate Rules
- General Data Protection Regulation (Chapter V)
  - Clear implementation of mechanism approved today
  - Safe Harbo(u)r is not listed – will it still be an option?
  - But: higher level of data protection inherent in the Regulation leads to higher requirements
  - Extra-territorial effect of the Regulation
Additional bureaucratic duties

- Annulment of the policy of compulsory registration is not relevant for Germany
- Internal data protection officers are already required in Germany (pursuant to the Regulation, it is only compulsory for companies to appoint a DPO if they employ more than 250 persons)
- Additional requirements contained in the General Data Protection Regulation:
  - strategies and measures (Article 22)
  - detailed documentation (Article 28)
  - notification and communication of personal data breaches (Article 31 and 32)
  - further obligations regarding data protection impact assessment (Article 33)
  - prior authorization and prior consultation (Article 34)
  - extended rights of the data protection supervisory authorities (Article 45 through 54)
## Stricter Sanctions

<table>
<thead>
<tr>
<th>Maximum penalty in % of global turnover</th>
<th>Offences include where a controller intentionally or negligently (Article 79):</th>
</tr>
</thead>
<tbody>
<tr>
<td>0,5%</td>
<td>• does not respond promptly or not in the required format to data subjects</td>
</tr>
<tr>
<td></td>
<td>• charges a fee for the information</td>
</tr>
<tr>
<td>1%</td>
<td>• does not provide the information in a sufficiently transparent manner or does not comply with the right to erasure</td>
</tr>
<tr>
<td></td>
<td>• does not react to objections filed by data subjects</td>
</tr>
<tr>
<td></td>
<td>• does not or not sufficiently maintain the documentation</td>
</tr>
<tr>
<td>2%</td>
<td>• processes data without a legal basis</td>
</tr>
<tr>
<td></td>
<td>• does not comply with the rules for international data transfers</td>
</tr>
<tr>
<td></td>
<td>• does not adopt appropriate internal guidelines</td>
</tr>
<tr>
<td></td>
<td>• does not designate an EU representative</td>
</tr>
</tbody>
</table>