Your Speakers

Dr. Annette Demmel, Berlin

Monika Kuschewsky, Brussels
Overview

- Introduction

- **Data Protection Impact Assessments** ("DPIAs")
  - Background
  - What?
  - When?
  - How to?

- Conclusion
The General Data Protection Regulation ("GDPR")

- 4 May 2016: Publication
- 25 May 2016: Date of entry into force
- As of 25 May 2018: Date of application

Including to companies that process personal data outside of the EU but offer their goods or services to individuals within the EU
GDPR and Data Protection Impact Assessments ("DPIA")

- GDPR introduces for the first time mandatory DPIAs (Art. 35)
  - No harmonised approach in the EU Data Protection Directive
    - Article 17 was limited to security
      - However: Were DPIAs implied through “prior checking” and “privacy by design”?

- Similar concept in Germany: prior checking ("Vorabkontrolle"), section 4d(5) of the Federal Data Protection Act

- Some national data protection authorities recommend privacy impact assessments
  - In particular the ICO in the UK

- See also the work of the Article 29 Working Party and data protection authorities outside the EU
  - In particular Canada, Australia, New Zealand
Non-compliance with the DPIA obligation

- Constitutes a serious violation, subject to a fine up to 10 million Euros or up to 2% of the total worldwide turnover of the preceding year

- May also lead to
  - Claims for damages
  - An order by a supervisory authority (SA)
  - Injunctions or interim measures by individuals or works councils
  - Loss of reputation and customer trust
What is a DPIA?

- A process to identify and reduce the privacy risks of new projects or practices
- An integral part of taking a privacy by design approach
- Difference to a privacy audit
  - DPIAs are prospective, act as an early warning system, may affect the design/end-result and are proactive
- Objectives
  - Minimizing risks
  - Preventing unlawful processing
  - Implementing privacy by design and by default
What triggers a DPIA?

- DPIAs shall be conducted, where
  - A **type** of processing is **likely** to result in a **high risk to the rights and freedoms of natural persons**
    - Taking into account: nature, scope, context and purposes of the processing
  - **Exemption** in Article 35(10)

- DPIAs are **particularly** required in the case of
  - Systematic and extensive evaluation based on automated processing, including profiling, and on which decisions with legal or similar effects are based
  - Processing on a large scale of sensitive data or of personal data relating to criminal convictions and offences
  - Systematic monitoring of a publicly accessible area on a large scale
  - Positive or negative lists by SAs
What is the content of a DPIA?

- The controller must assess the **impact** of the envisaged processing operations on the **protection of personal data**

- **Minimum content**
  - Systematic description of the **processing** and its **purposes**
    - Including, where applicable, the legitimate interest pursued by the controller
  - Assessment of the **necessity** and **proportionality** of the processing
  - Assessment of the **risks** to the rights and freedoms of data subjects
    - Consider expectations of the individuals
    - Evaluate the level of risk, based on likelihood, and impact
  - The **measures envisaged** to address the risks
    - Including safeguards, security measures and mechanisms (e.g., pseudonymisation, anonymisation, encryption, local storage, access restriction, limiting retention)
    - Compliance with approved codes of conduct shall be taken into account

- **Documentation**
When to conduct a DPIA?

- **Time** of conducting it
  - **Prior** to the processing

- **How often** to conduct it
  - **A single assessment** may **suffice**
    - If it addresses a set of similar processing operations that present similar high risks
  - **A review** may be **required**
    - At least when there is a change of risk
Typical procedure

PIA

Consultation / Analysis → Preparation → Documentation / Reporting → Follow-up → PIA
Who must be involved?

- **Data Protection Officers** (“DPOs”)
  - Controllers shall seek the DPO’s advice
  - DPOs shall provide advice and monitor the performance of the DPIA

- **Data subjects** or their representatives, where appropriate

- **Supervisory authorities**
  - See next slide

- Assign responsibility internally
Role of the SAs

- Establish **positive** and **negative lists**
- **Prior consultation** of the SA in case of high risk in the absence of mitigation measures
  - If intended processing is considered to infringe the GDPR, SA shall provide **written advice** to the controller (or the processor) within eight (may be extended by another six) weeks and may use any of its powers
  - When consulting the SA, the controller shall provide the SA with the DPIA and
    - the **respective responsibilities** of the controller, joint controllers and processors involved in the processing
    - the **purposes** and **means** of the intended processing
    - the **measures** and **safeguards** provided to protect the rights and freedoms of data subjects
    - where applicable, the **contact details** of the DPO and
    - **any other information requested** by the SA
Recommendations

- Await guidance from the Article 29 Working Party and the positive/negative lists from the SAs

- Eventually conduct “DPIAs light”, irrespective of legal obligation

- Consider DPIAs as more than mere legal compliance and integrate them in your overall risk management practice
Conclusion

- A DPIA is not the end: it is an (ongoing) process
Questions and Answers
Thank you!

Dr. Annette Demmel
Partner, Berlin
Rechtsanwältin
Certified Specialist for Information Technology Law
Certified Specialist for Copyright and Media Law

Monika Kuschewsky
Partner, Brussels
Rechtsanwältin
Certified Information Privacy Professional/Europe (CIPP/E)
Betrieblicher Datenschutzbeauftragter (GDDcert.)

annette.demmel@squirepb.com
monika.kuschewsky@squirepb.com