The Future of Data Privacy in Europe

THE EUROPEAN GENERAL DATA PRIVACY REGULATION (GDPR)

KLAUS-E. KLINGNER - GSEC GWAPT CDPS

About Me ...

Klaus-E. Klingner

- Certified Data Security Professional (GSEC)
- ISO27001 Implementor
- Certified Web Application Pentester (GWAPT)
- Certified Data Privacy Specialist (CDPS)
- Veterinarian, Beekeeper

May 25th 2018

A new Age of Data Privacy

The Future of Data Privacy in Europe

- Data Privacy in the European Union
- The New European General Data Protection Regulation
- Keypoints of the new GDPR
- Application to International Organisations
- Processing of Data by (international) Third Parties

Data Privacy in the European Union

- 28 Countries
- 28 Legislations
- > 200 Laws and Regulations applying to Data Privacy just in Germany

Time for a Common Data Privacy Regulation

- Oct. 1995 – The European Data Protection Directive (Directive 95/46/EC)
- Jan. 2012 – Proposal for a comprehensive reform
- July 2015 – Recommendation for the final text of the GDPR
- Dec 2015 - EP, Council and EC reach an agreement on the GDPR
- May 24th 2016 - The Regulation enters into force, 20 days after publication in the Official Journal of the EU
- May 25th 2018 – The GDPR applys in all countries of the Eropean Union

Application to International Organisations

- Processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
- Offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union
- Monitoring of data subjects' behaviour as far as their behaviour takes place within the Union
- Contract with a client from within the EU or a client applying GDPR

Source : https://www.kentico.com/blog/gdpr-and-non-eu-companies-where-is-the-line-drawn

To whom it may concern …

- Every national governmental organisation in the EU
- Every european organisation or business
- Every organisation or business outside the EU offering services to, doing business with, or collecting data of european residents

Keypoints of the new GDPR (1/3)

- Severe Penalties for Breaches:
  - Maximum of 4% of annual Global Turnover or €20 Mio.
- Definition of Personal Data now includes digital identifiers
  - IP Adress
  - Mobile Device Identity
- Explicit Consent from Individuals required (if no legal base)
  - Voluntary
  - Specific
  - Informed
  - Unambigous
  - statement or clear affirmative action

Keypoints of the new GDPR (2/3)

- Clearly Defined Rights of the Individual
  - The Right to Information
  - The Right to Correctness
  - The Right to Transfer
  - The Right to be Forgotten
- Technical and Organisatory Measures (TOMs)
  - Confidentiality – Integrity – Availability
  - Auditable by Regulator

Keypoints of the new GDPR (3/3)

- Record of personal data processing activities (Data Processing Registry)
  - Data Lifecycle
  - Responsible Data Controller
- Data Privacy Impact Assessments
- Mandatory Reporting of Personal Data Breaches within 72h
- Appointment of a Data Privacy Officer

GDPR and Webportals

- You must provide notice BEFORE any data is collected
  - Clear and concise
  - What data is collected and how is it used
  - Easily accessible (Privacy Notice – Cookie Notice)
- You must receive consent BEFORE data is collected or identifying cookies are placed
  - Easily accessible
  - Revocable
  - Inaction cannot be considered consent
- You may be LEGALLY RESPONSIBLE for data collection that occurs without your consent
  - Tag manager
  - Vendor piggybacking

Processing of Data by (international) Third Parties

- Data Processing Agreement
  - Shared Responsibility
  - European Standards for Data Privacy or Equivalent guaranteed
- European Model Clauses
- Binding Corporate Rules (BCR)

Summary

- The new Regulations will be in Force starting May 25th 2018
- One Regulation for all Members of the EU
- Applys to any Organsiation offering Services to European Residents
- Stricter Obligations for Organisation and Businesses
- Rights of the Individual strengthened
- Severe penalties for non-compliance and breaches

More Information

Full Text of the GDPR:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Thank You for Your Attention

Klaus-E. Klingner
klingner@silverday.de