Data Protection Certification for Cloud Services

Prof. Dr. Georg Borges

Berlin, 13th December 2016
Trusted Cloud: Legal Framework of Cloud Computing

- **Pilot Project „Data Protection Certification for Cloud Services“** (2013-2016)
- Data protection authorities, businesses, associations
- **Topics**
  - Certification requirements for cloud services
  - Certification process for cloud services
- **Step 1 (2013 – 2015)**
  - Framework for certification
  - Trusted Cloud Data Protection Profile (TCDP) 0.9
- **Step 2 (2015 – 2016)**
  - Pilot certification of cloud services
  - Trusted Cloud Data Protection Profile (TCDP) 1.0
Compliance certification in the field of data protection

Challenge: Supervision of cloud service providers by cloud users
- Art. 17 Data Protection Directive / § 11 German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)
  - Assessment of technical and organizational measures
  - Cloud user does not have sufficient knowledge to analyze the measures
  - On-site inspection by every cloud user is inefficient

Solution: data protection certification for cloud services
- Inspection of cloud service carried out and certified by an independent third party with appropriate qualification
- Inspection by cloud user substituted by certificate
Elements of compliance certification for cloud services

Uniform requirements for certification

**Trusted Cloud Data Protection Profile for Cloud Services**

- Specifies the legal requirements of German Federal Data Protection Act / European Data Protection Directive
- Based on ISO/IEC 27002 / 27017 / 27018
- Takes different levels of protection requirements into account
- Published in April 2015 as TCDP 0.9
- Implemented and tested in 2015 /2016
- Published in September 2016 as TCDP 1.0
Elements of compliance certification for cloud services

Uniform certification procedure

Rules of Procedure for Certification According to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP)

- Requirements for auditors and certification bodies
- Rules for assessment of cloud services
- Rules for certification of cloud services
- Take into account GDPR provisions
- Published in September 2016
Elements of compliance certification for cloud services

Efficiency of data protection certification

- **Separate levels of security**
  - Challenge: Different levels of security required in practice
  - Solution: Certification according to security levels
  - Different security levels set out in TCDP
  - Security levels as part of the certificate
Elements of compliance certification for cloud services

Efficiency of data protection certification

- **Modular certification concept**
  - Separate certification of different modules of a cloud service
  - Single certification of module for multiple services
Certification of cloud services and GDPR

The General Data Protection Regulation and certification

- Certification as a means for demonstrating compliance, Art. 28 V
- Requirements for certification procedure in Artt. 42, 43

Future tasks for certification of cloud services

- Developing a certification standard based on GDPR
- Seeking recognition of the standard by the Board, Art. 42 V
- Adaptation of the certification procedure to the GDPR
Perspective: German-French Initiative on European Cloud Certification

Potential of a German-French Cooperation

- Creating a common standard for certification of cloud services
- Creating a framework for certification procedures
- Certification of cloud services for the entire internal market
- Potential for a globally recognized standard of data protection certification
Thank you very much for your attention!

More Information: www.tcdp.de

Prof. Dr. Georg Borges
Chair of Civil Law, Legal Informatics, German and International Business Law and Legal Theory
Institute of Legal Informatics – Saarland University

+49 (0)681 / 302-3105
georg.borges@uni-saarland.de

www.rechtsinformatik.saarland