STANDARDS TO HELP COMPLY WITH EU LEGISLATION.
EUROPE HAS WHAT IT TAKES – INCLUDING THE WILL?

Presented by Helmut FALLMANN
HOW DATA PROTECTION AND CYBER SECURITY DETERMINE CLOUD PENETRATION
Cloud Penetration Depends on Data Protection and Cyber Security

- Europe has implemented major reforms in the area of data protection (GDPR, NIS).
- We could become a role model for the rest of the world.
- If the existing restrictions are eliminated, a competitive Single Market for secure, reliable and convenient Cloud Services could emerge in the EU.
STRATEGIC TRACKS
IN ORDER TO LEVERAGE
THE POTENTIAL OF THE CLOUD
How to Leverage the Potential of the Cloud

  - Cutting through the Jungle of Standards
  - Safe and Fair Contract Terms and Conditions
  - European Cloud Partnership to drive innovation and growth from the Public Sector
- C-SIG developed “EU Code of Conduct for Cloud Service Providers” (CoC).
- Submission of report “Establishing a Trusted Cloud of Europe” (2014).
Provenance and Timeline
EU Data Protection Code of Conduct

European Commission Cloud Strategy
Cloud Select Industry Group founded
First draft industry code (all stakeholders)
Code matures – Art 29 WP input
EU CoC General Assembly (Feb 2017 Alibaba Cloud, Fabasoft, IBM, Oracle, Salesforce and SAP)
GDPR in force

2012 2013 2014 2015 2017 2018

© ETSI 2018 - All rights reserved
STREAMLINING OF CERTIFICATION ACTIVITIES TO THE DSM
Overall Picture and Next Steps

- The Cybersecurity Act (CSA) establishes the European cybersecurity certification framework as *lex generalis* (Art. 1).
- The Cybersecurity Act foresees that ENISA shall prepare a candidate security certification scheme for specific ICT products or services in accordance with the requirements of the CSA. This requires a consultation of relevant stakeholders.
- The fast development of a candidate certification scheme for cloud computing is crucial for cloud uptake and the free movement of data in Europe.
Together CSIG-Cert and the European Union Agency for Network and Information Security (ENISA) delivered a list of (voluntary) certification schemes for the cloud (CCSL) to give potential cloud customers more transparency about certification schemes and how they relate to the cloud.

As an extension of the CCSL, CSIG-Cert and ENISA also delivered the Cloud Certification Schemes Metaframework (CCSM) in order to facilitate the use of existing certification schemes during procurement of cloud services. It provides a neutral, high-level mapping of potential customers' security requirements to security objectives in existing cloud certification schemes.
ISO 27001 & ISO 27018

• Information security and protection of personal data
• Globally recognised standard for the assessment of the security of IT environments
• Compliance with clearly defined technical and security based standards
• Defined data protection requirements for CSPs
• Addresses Business Continuity Management (BCM)
ISAE 3402 Type II

• International Standard on Assurance Engagements
• International testing standard that assesses the effectiveness of internal control systems of service providing organisations
• Tests extensively an organisation’s internal control system and rates its effectiveness in detail
EuroCloud Star Audit

- Detailed check of contracts and SLAs
- Certification system based on best practice
- Carried out by EuroCloud Europe
- Focus on security and compliance with data protection within a Cloud environment
- Comprehensive and entirely disclosed list of criteria
- Fabasoft is the only company worldwide to receive five stars for its Cloud Service.
Cloud Computing Compliance Controls Catalogue (C5)

- Controls catalogue issued by the German Federal Office for Information Security (BSI)
- Recommendation for procurement
- Specifies the minimum requirements for CSPs
- Most comprehensive catalogue of much more than 100 criteria, which have to be included into CSP’s SLAs
- Fabasoft is the first European Cloud Service Provider to have received the attestation.
ANSSI SecNumCloud

- Controls catalogue issued by Agence nationale de la sécurité des systèmes d’information (ANSSI) based on ISO 27001
- Defines minimum requirements for cloud IT service providers for IaaS, PaaS and SaaS
- Goal: give assurance regarding competencies and service quality of Cloud Services
- Two approval levels (Essential, Advanced)
- Close cooperation between ANSSI and BSI to achieve the same level of security
Streamlining of Certification Activities

• Result stakeholder survey: European Commission should harmonize corresponding standards and applicable law based on existing certification schemes.

• DSM Cloud Stakeholder Group has started two working groups:
  • WG on a candidate cloud security certification scheme
  • WG on a code of conduct for data porting and cloud switching (with subgroups for IaaS and SaaS)
Benefits of Cloud Security Certifications for Customers

- Trust based on European regulation
- Higher quality in terms of security and privacy than usually provided by customer’s internal IT
- Basis to create new innovative digital services to support digital transformation
Value of Certifications for CSPs

• Certifications have to be included in standard requirements for procurement of Cloud Services.

• **Example:**
  Cloud Computing Compliance Controls Catalogue (C5) is recommended by BSI as a minimum standard for the adoption of Cloud Services in the public sector in Germany.
Key Objectives for Building a European Data Economy

• EU Data Protection Code of Conduct for cloud service providers including a European scheme for Data Protection Certification (GDPR)

• Code of Conduct for data porting and cloud switching for IaaS and SaaS (Cybersecurity Act)

• European Scheme for Cloud Security Certification (Cybersecurity Act)
THE CHALLENGES AHEAD:
NATIONAL BORDERS,
ADEQUACY DECISIONS AND GLOBAL STRATEGY
(New!) National Borders

• Example: Stiftung Warentest
• Mandatory requirements for online shopping at www.test.de:
  • Place of residency: Germany
  • Instrument of payment has to be German
Adequacy Decisions and Global Strategy – Example: The Case of Facebook

- Facebook was no longer concerned with what happened to user data once it left its servers.
- Yet if there had been a recognised independent authority that prohibits such practices then incidents on the scale of the current Facebook scandal would have remained unthinkable!
- The case clearly shows the advantages of the European value system with a strict and rigid data protection regime.
THANK YOU FOR YOUR ATTENTION!