ETSI Summit, Releasing the Flow

Regulation, Self-Regulation and Technical Standards for Data Protection, Data Security and Data Portability

Pierre Chastanet

Acting Head of Unit Cloud & Software

DG CONNECT, European Commission

19-April-2018

Cloud & Data Technologies
Regulation vs. Self-regulation

Regulatory challenges for Cloud Computing

- **Fast development of technologies**
- **Regulatory framework developed for "static" environments, not necessarily fit for "dynamic" ICT environments !**
- **Current regulatory environment does not facilitate the uptake of cloud and data technologies !**
- **Different policy areas or activities → Complexity**

Cloud & Data Technologies Regulation vs. Self-regulation

Regulatory objectives for Cloud Computing

- **Appropriate regulatory environment**
- **Foster investment, innovation and cloud transformation**
- **Preserve important public values**

Guiding principles of Self-regulation

- **Balanced and relevant participation**
- **Openness, Inclusiveness and Transparency**
- **Good faith, Commitment and Constructiveness**
- **Clear and Unambiguous Objectives**
- **Legal Compliance**

Cloud Data Protection Codes of Conduct (CoC)

*The EC supports **self-regulatory initiatives**, which: –*

- *aim at facilitating the proper application of data protection laws in the specific context of cloud computing services*
- *promote trust and legal certainty*

- *Art.27 of **Directive 95/46/EC**: approval by the Working Party 29 required*
- *Art. 40 of the **GDPR**: approval by the DPAs (1MS) and the European Data Protection Board (EDPB) required*

- *3 Data Protection Codes of Conduct for Cloud Computing*
  - **EUCoC (IaaS, PaaS, SaaS)**
  - **CISPE CoC (IaaS)**
  - **CSA CoC (IaaS, PaaS, SaaS)**

Hybrid Approach
Best practice in the FFD Proposal

- **Principles-based**, not detailed (Better Regulation):
  - **The free movement of non-personal data principle**
    - 'public security' – the only exception
    - notifications and transparency for effective implementation
  - **The principle of data availability** for regulatory control by competent authorities
    - supported by cooperation between competent authorities through single points of contact
    - fall-back approach – if there is no specific applicable cooperation mechanism

Hybrid Approach
Best practice in the FFD Proposal

- **Important role for self-regulation**
  - Promoting development of **self-regulatory codes of conduct for easier switching of provider and/or porting data** back to in-house servers

- **Cross-dependency with Cyber Security Act**
  - **Security and trust enabler for Free Flow of Data**

Switching Providers & Porting Data

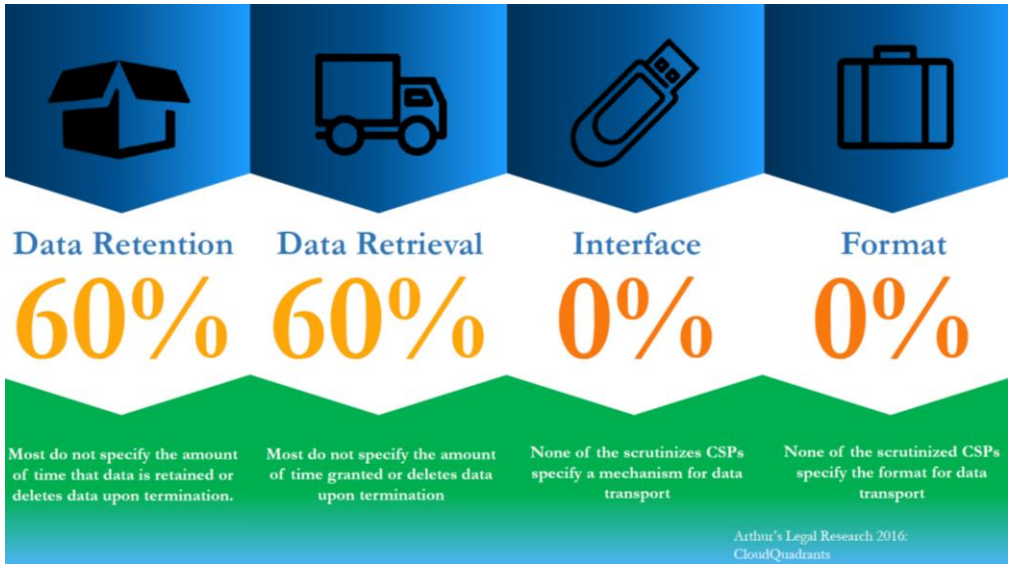
THE VENDOR LOCK-IN PROBLEM:

- Digital Single Market strategy, 2015: Vendor lock-in leads to trust problems around cloud adoption.

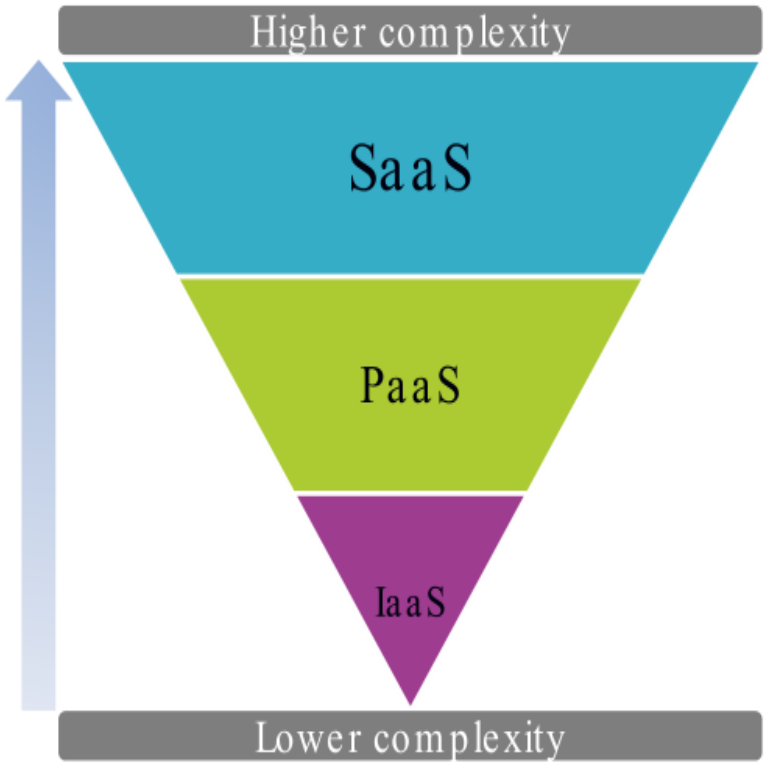
- Study "Switching of Cloud Service Providers" (in progress):

- The public consultation on building a European data economy (2017):

- **72% of business users of Cloud intends to switch providers;**
- **45% of those experiences problems with switching;**
- **56.8% of SMEs experiences problems with switching.**



Complexity of porting/switching



- Data interdependencies tend to increase with :
  - type of cloud service consumed: higher complexity in SaaS versus IaaS
  - size of organization
- Data portability works if vendors:
  - are transparent about: data model / data schema /data semantics
  - build services based on open standards APIs and protocols for data movement

Switching of Cloud Services Providers (SMART 2016/0032)

"SWIPO":

Self-regulatory Codes of Conduct for Switching Cloud Service Providers

Article 6 of Free Flow of Data Proposal:

- **"The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level, in order to":**
  - Define best practices
  - Define information requirements

  → Deadline: 1 year after start of application, review after 2 years. Follow-up actions?

Process:

- **Self-regulatory (Commission is observer)**
- **Open & inclusive process (open call)**
- **Initially 2 Codes: IaaS / SaaS (2 sub-WGs)**
- **Balanced representation: 6 co-chairs suggested by the Commission**
- **Qualification criteria for involvement: experience & expertise.**

→Process launched on 12 December 2017.

→First meeting of the WGs: 17 April 2018.

Cloud Security Certification

- **6 billion** devices will be connected to the internet by 2020 in the EU and **threats are increasing!**

CLOUD AT THE CORE !

- ✓ Proposal for a **EU Cybersecurity Act, including the reform of ENISA and towards a European Cyber Security Certifications Framework**
- ✓ **Cloud security is a prerequisite for enabling the Free Flow of Data in the EU and promoting Cloud uptake**
  - → **WG on Cloud Security Certification is exploring the possibility of developing a candidate European Cloud Security Certification Scheme**
  - → **European Cloud Security Certification Scheme will promote scale-up of EU CSPs**

Security Standards and industry-led Cloud Certification schemes

International Organization for Standardization

ISO/IEC 17203, ISO/IEC 17826:2012, ISO/IEC 19041, ISO/IEC 19044, ISO 19086, ISO/IEC 19099, ISO/IEC 19831, ISO 19941, ISO 19944, ISO/IEC 20000-1, ISO 22301,ISO/IEC 24760-1, Family of ISO/IEC 2700x, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115.

OASIS TOSCA, OASIS CAMP

NIST SP 500-299, Draft NIST SP 500-307, NIST SP 800-125, NIST SP 800-144

CSA CCM, CSA CTP, CSA A6, CSA CAIQ, CSA TCI, CSA PLA, CSA Attestation - OCF Level 2, CSA Attestation - OCF Level 1, CSA Self-Assessment - OCF Level 1

SNIA CDMI, DMTF DSP0243, DMTF DSP0263

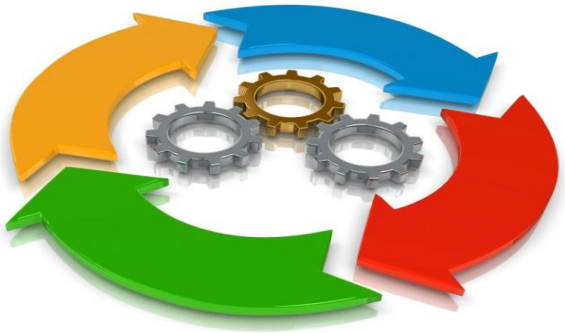
EuroCloud Self-Assessment, EuroCloud StarAudit EuroCloud ApprovedDC

ITU-T X.1601, ITU-T X.1631

AICPA SOC 1, AICPA SOC 2, AICPA SOC 3

Others

European Commission proposal for a Cybersecurity Certification Framework



*This will enable the creation of sectorial EU certification **schemes** for ICT products and services…*

*…that are **valid across the EU***

Cloud could be one of those schemes

Conclusions

- *Regulation to:*
  - **Provide legal certainty**
  - **Set core principles**
- *Codes of Conduct, Standards and Certification to:*
  - **Foster trust in cloud-based services**
  - **Increase geographical and vendor mobility of data**
  - **Ensure practical implementation of data protection and cybersecurity requirements**
  - **Importance of industry mobilisation (users/providers)**
- *Data protection and cybersecurity certification convergence?*

European Commission