TIMELEX

LEGAL ASPECTS OF CLOUD COMPUTING

Cybersecurity Coalition

Webinar Series

22 June 2020

AGENDA

1. When does a service become a“cloud computing services”?

2. Confidentiality and cloud computing services

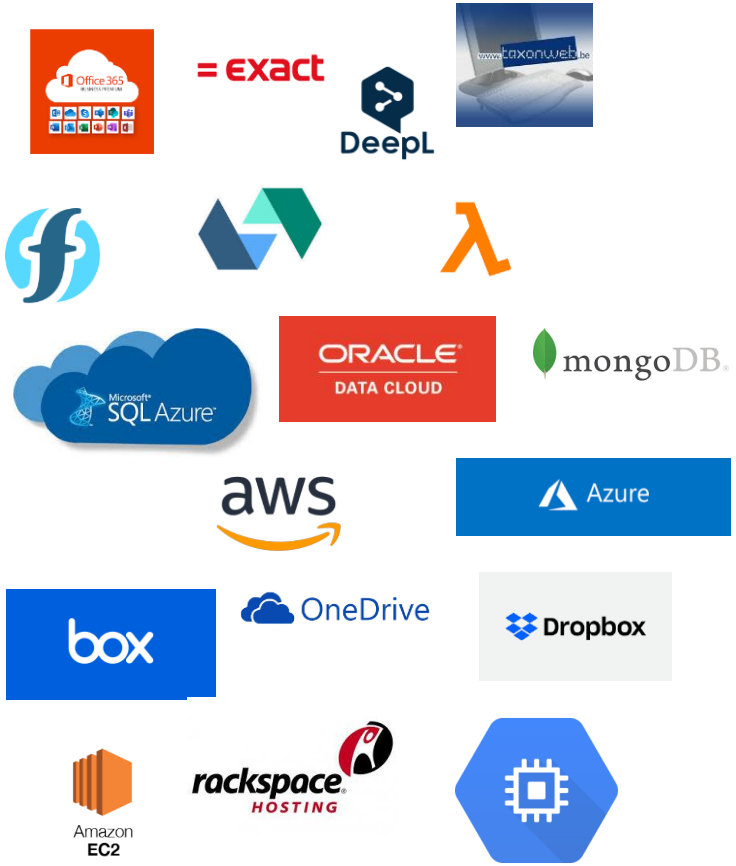
TIMELEX

WHEN DOES A CLOUD SERVICE BECOME A "CLOUD COMPUTING SERVICE"?

Applying a legal definition in practice

WHEN WE THINK ABOUT CLOUD SERVICES

Deployment model	Service delivery model
Private cloud	SaaS
	FaaS
Community cloud	DaaS
	PaaS
Public cloud	STaaS
	IaaS
Hybrid cloud	



DEFINING CLOUD COMPUTING SERVICE

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction

NIST SP 800-145 (2011) "The NIST Definition of Cloud Computing"

Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

ISO/IEC 17788:2014 (2014) "Information technology — Cloud computing — Overview and vocabulary"

TIMELEX

CLOUD COMPUTING SERVICE

A digital service…

- […] allowing access
  - NOT electronic communications service (expressly excluded)
- […] to a scalable and elastic pool
  - Scalable = computer capacity allocated by cloud computing service providers in a flexible manner, irrespective of the geographic location of the capacity, in order to cope with fluctuations in demand. **Look at scalability from the provider's perspective, not the user!**

    In other words: the ability to make a system *larger* (i.e. easily have additional tasks done without impact on performance; cf. vertical and horizontal scaling)
  - Elastic = the degree to which a system is able to autonomously adapt to changes in workload by deploying more or less resources.
- […] of shareable computing capacity
  - computer capacity made available to several users who have a common access to the service, but where the processing is carried out for each user separately
  - capacity such as networks, servers and other infrastructure, storage, applications and services

GREAT… SO?

Online repository of manuals

Google Translate

Zoom Video Calling

E-banking portal

Office 365

Private cloud-hosted ERP

FAS

Customer Portal

Auth0

Darktrace

A PAN-EU PERSPECTIVE

- The Netherlands:
  - *Wet beveiliging network- en informatiesystemen*
  - Look at service delivery model: IaaS, PaaS and SaaS are all cloud services
  - Private cloud is **not** a “digital service” (?)

- Belgium
  - *Wet tot vaststelling van een kader voor de beveiliging van network- en informatiesystemen van algemeen belang voor de openbare veiligheid*
  - Definition NIS-Directive, no further clarification given
  - CCB: refers to the clarification given

- UK
  - *Networks and Information Systems Regulations 2018*
  - “The Government considers that this would likely exclude most online gaming, entertainment or VOIP services, as the resources available to the user are not scalable, but may include services such as email or online storage providers, where the resources are scaleable.”
  - “DCMS considers that in order for a DSP to be in scope of NIS, they have to provide their services to external bodies or customers.

- France
  - *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*
  - No specific clarifications given
  - Law follows the definitions of the Directive

TIMELEX

CONFIDENTIALITY AND CLOUD COMPUTING SERVICES

When your cloud vendor is (not) allowed to know…

TYPOLOGY OF CONFIDENTIALITY OBLIGATIONS

1. Contractual confidentiality obligation
   - A. Purely contractual basis
   - B. Typically confidentiality level “orange” or “red”
   - C. No right to remain silent in a court of law
   - D. Infringements only enforced through civil law mechanisms
2. Duty to discretion
   - A. Statutory/pseudo-statutory obligation “Need-to-know”
     - 5.1 (f) GDPR for every controller processing personal data
     - 318 WIB for financial institutions
     - Auditors, accountants, tax advisors as part of their deontology
     - Members of the board in a limited liability company
   - B. Typically confidentiality level “orange” or “red”
   - C. No right to remain silent in a court of law
   - D. Infringements typically not penalised under criminal law (but civil law liability or administrative sanctions are possible)
   - E. Relationship “holder” and “service provider” not explictly governed
3. Professional secrecy
   - A. Statutory obligation (explicit legal basis)
     - Art. 458 Criminal Code
     - Art. 9 NIS-Act
     - Art. 58 of the Act of 22 April 1999 regarding the accounting and tax professions
     - Art. 86 of the Act of 7 December 2016 on the organisation of the profession of and the public supervision of statutory auditors
   - B. Confidentiliaty level “red”
   - C. Right to remain silent in a court of law
   - D. Infringements are penalised (Art. 458 CC)
   - E. Obligation of professional secrecy also applies to anyone for whom the “holder” is responsible

CONFIDENTIALITY OBLIGATIONS OF THE DSP

- Often governed purely on a contractual basis
  - NDA
  - confidentiality clauses in service agreement, sometimes sharpened/extended through DPA or addenda
    E.g. Microsoft Cloud Agreement Professional Secrecy Amendment
- Parties decide themselves how to shape confidentiality obligations, typically includes:
  - Confidentiality throughout the contractual chain;
  - Relationship with IAM measures;
  - Traceable and auditable confidentiality (logging);
  - Reporting obligations in case of breach;
  - Notification obligations in case of governmental or judicial access requests;
  - Extreme (e.g. Crossroad's bank social security policy guidelines on cloud) -> sovereignty clause
- Typical carve-outs include:
  - to prepare or bring a claim or defense;
  - to comply with an order from competent law enforcement, judiciary or other governmental authorities;
  - when information was already known through other channels.

PROFESSIONAL SECRECY IN THE CLOUD

Professional secrecy ≠ contractual confidentiality

-> contractual carve-outs are not acceptable

Cloud vendor himself subject to professional secrecy obligations

-> applicability Art. 458 Criminal Code

Important: alert cloud vendor AND contractual acknowledgement

-> will not work in case of foreign governmental access requests

-> technical measures crucial (data localization (?), encryption, key management with principal, etc.)

THE SPECIAL CASE OF CLOUD SECURITY VENDORS (1)

- Art. 9, §2 NIS-Act:

  "The staff of an operator of essential services, a digital service provider, or their subcontractors, shall be bound by professional secrecy as regards information relating to the implementation of this Act.

  Persons who, by virtue of their state or profession, have knowledge of secrets entrusted to them, may disclose these secrets for the implementation of this law."

- Art. 51, §8 NIS-Act:

  "Infringements of Article 9 §§ 2 and 3 of this Act are punishable by the penalties provided for in Article 458 of the Criminal Code."

Security of systems and facilities

Systematic management
- Mapping information systems (i.e. infrastructure and landscape)
- Appropriate policies incl. risk analysis, HR, security of operations, security architecture, secure data and life cycle management, encryption management where appropriate

Physical and environmental security
- All-hazards risk-based approach
- Measures aimed at addressing system failure, human error and natural phenomena

Security of supplies
- Appropriate policies to ensure accessibility and traceability of critical supplies

Access controls
- Physical and logical access control is administrated based on business requirements

Incident handling

Detection processes and procedures

Incident reporting and weakness/vulnerability identification

Established response procedures and result reporting

Incident severity assessment, documenting knowledge, evidence collection, continuous improvement process

Business continuity management

Implementing contingency plans based on business impact analysis

Disaster recovery capabilities which are tested

Monitoring, auditing and testing

Assess whether network and information systems work as intended

Audit whether standards and guidelines are complied with, records are accurate and targets are met

Implement process to detect security flaws

Compliance with international standards

THANK YOU

Questions?

Timelex

Rue Joseph Stevens | Joseph Stevensstraat 7
B-1000 Brussel

ruben.roex@timelex.eu

(t) +32 (0)2 893 20 95

info@timelex.eu
www.timelex.eu