Enabling Privacy and Security for Data Outsourced to the Cloud

Pieter-Jan Ombelet
KU Leuven Centre for IT & IP Law
TDW Conference, The Hague
CLARUS
A Framework for User Centred Privacy and Security in the Cloud

http://clarussecure.eu
contact@clarussecure.eu
@CLARUSecure
What is the focus of CLARUS?

CLARUS implements a holistic security-by-design approach to overcome mistrust in cloud computing

• A secure **proxy-based solution** for the storage and processing of data outsourced to “honest-but-curious” cloud service providers (CSPs)
• New **privacy-preserving mechanisms** (encryption, anonymisation, splitting/merging) to protect sensitive data outsourced to the cloud
• Monitoring and auditing services to give users control over outsourced data
• An **interoperability-by-design** approach to overcome mistrust by implementing standardised cloud services
• A comprehensive analysis of the EU legal framework for the protection of sensitive data
CLARUS solution

Proxy located in the trusted domain that continuously manages privacy, trust and security as system properties

- **Privacy** -> Privacy-enabling mechanisms to protect users’ sensitive data outsourced to the cloud
- **Trust** -> Auditing services to give users control on how data are protected while outsourced to the cloud
- **Security** -> Attack tolerant framework to dynamically detect and mitigate security breaches

CLARUS is demonstrated in two case studies

- e-Health
- Geo-referenced data
Data Protection Directive

- Summary of the key principles
General Data Protection Regulation

**GDPR**
- Replaces the national implementations of the Data Protection Directive (95/46/EC)
- Harmonises the data protection legal framework
- Affects all companies operating business within the EU

**Impact**
- Enhances individuals’ rights
- Strenghtens companies’ obligations
- Increases sanctions in case of non-compliance
Key changes

- Single set of rules: exception for eHealth
- Broader scope
- New definitions: e.g. pseudonymization, health data
- Consent and legitimate interest
- Data subject’s rights are enhanced
- Accountability – Privacy by Design and by Default
- Data breach notification
- Strengthened enforcement and huge fines
Privacy by Design

- Proactive not reactive, preventive not remedial
- Privacy as a default
- Privacy embedded into design
- Full functionality: positive sum not zero sum
- End to end security: lifecycle protection
- Visibility and transparency
- Respect for user privacy

Foundational Principles
A disruptive technology for the market

Cloud Service Providers will gain the trust and confidence of customers by offering user- and privacy-friendly services leveraging CLARUS.

Citizens will no longer need to be wary of their sensitive data being leaked when stored and managed by CLARUS-enabled clouds.

The health sector benefits from a more efficient, transparent and standardised auditable cloud services to protect the patient records outsourced to the cloud.

Geospatial providers have the right tool to protect privacy and to increase users’ trust in their location-based services.

CLARUS innovative solutions reinforce trust and security in digital services for handling personal data (action 12 of DSM strategy).
Identified future challenges

• Develop more protocols to be able to perform more operations on split, anonymised and encrypted data directly in the cloud.
• Implement the CLARUS platform and deploy it in the two case studies.
• Ensure the developed platform can easily be adapted to other case studies
• Ensure the developed platform’s compliance with the General Data Protection Regulation.
Contact details

• For legal questions: Pieter-jan.ombelet@law.kuleuven.be
• For technical questions: josep.domingo@urv.cat, david.sanchez@urv.cat