Towards Trust in cloud services with CLARUS – how we are tackling related legal issues

Pieter-Jan Ombelet (KU Leuven), Stephanie Mihail (KU Leuven), March 2016

Focus Area

The aim of the Horizon 2020 CLARUS project is to offer cloud services that are compliant with global standards and European IPRs reflecting federated and coherent roadmaps. CLARUS will impact the current cloud landscape by delivering key elements spanning reinforced European leadership in privacy-preserving technologies by safeguarding the privacy of citizens in cloud computing environments, increased interoperability of systems and services from different vendors and innovative research in security-enabling techniques and new architectures for secure delivery in the cloud. This paper provides an overview of the legal research that is undertaken within the context of CLARUS, with a particular focus on the legal issues encountered during the development and deployment of the CLARUS solution.

Who benefits and how?

More specifically, CLARUS will enhance trust in cloud services by developing a secure framework for the storage and processing of data outsourced to the cloud. The CLARUS framework aims to allow end users to monitor, audit and retain control of the stored data while maintaining the functionality and cost-saving benefits of cloud services.

Tackling legal challenges

The main legal concerns impeding the mainstream adoption of the cloud relate to privacy and security matters, as well as the concepts of interoperability and portability. In this respect, multiple legal frameworks are analysed.

First and foremost, the development of CLARUS draws on the use of two distinct data sets, namely geospatial data and eHealth data. The first data set relates to freedom of information legislation, whereas the second data set is analysed under the EU privacy and data protection framework. In Europe, legislation on freedom of information is rather fragmented and divergent. Despite differences, there are two clear exceptions regarding access related to environmental and spatial data of particular significance in relation to the geospatial data used for the CLARUS project. More specifically, the EU has established a clear legal framework vis-à-vis the availability of public sector spatial data. There are three main Directives, namely the ACCESS Directive, INSPIRE Directive and PSI Re-use Framework.

Legal research for the eHealth use case has a clear focus on privacy and data protection issues, as one of the priority areas for CLARUS. The legal requirements of the current data protection legislation, as well as the upcoming and recently adopted General Data Protection Regulation (GDPR), are thoroughly analysed for the implementation of a legally compliant CLARUS solution. Attention is paid

to the concept of 'Privacy by Design' and the associated challenges for its implementation, as well as to the consequences and implications of the 'Safe Harbor' decision on the transfer of personal data.

Regarding the security aspects relevant to CLARUS, we have explored the liability issues of cloud service providers and intermediaries, based on the general tort law and the E-commerce Directive. Certain relevant cybercrime legislation and EU Directives on attacks against information systems are also analysed, as well as the European Investigation Order in criminal matters.

The added value of the CLARUS solution lies in enabling the delivery of new and improved services, while retaining full control over any potentially confidential or business-critical data outsourced to the cloud. For cloud service providers, the CLARUS trust-enabling solution will increase market potential by attracting a much broader spectrum of prospective cloud customers . These objectives will also be met by making a thorough analysis of the key elements of the applicable legal framework alongside the study of the recent milestone decisions.

The comprehensive legal guidance on the impact of these legal requirements in cloud services will enhance the trust of all stakeholders, particularly organisations on the demand side currently reluctant to adopt cloud services. In addition, this research will bring further concrete recommendations for partners and policy makers to ensure a fully compliant CLARUS solution that could improve user's trust, safety, privacy and confidence in cloud services.

www.clarussecure.eu | @CLARUSecure