Assessing IT Security Standards Against the Upcoming GDPR for Cloud Systems

Cesare Bartolini, Gabriela Gheorghe, Andra Giurgiu
Mehrdad Sabetzadeh, Nicolas Sannier
{*firstname.lastname*}@uni.lu

The protection of personal data has seen a major upheaval in the last years, with a growing attention from legislators, entrepreneurs, developers, authorities and the general public. This is related to the increasing adoption of cloud-based services, and the focus on personal data as a pivotal asset in modern business models. The fact that personal data have a significant monetary value is proven by the emergence of many "free" services. The benefit for a company providing such services (and possibly its only source of income) stems from processing such personal data, especially selling them to third parties.

The main EU legal instrument that sets the general rules for the processing of personal data is Directive 95/46/EC, which gives Data Subjects (DSs) a set of rights with respect to such processing, states the obligations controllers and processors have to comply with when dealing with personal data and foresees oversight authorities and mechanisms meant to safeguard adherence to these rules. The same general rules apply when data is stored or otherwise processed in the cloud. However, the fast-paced evolution of technology over the last two decades has exposed several weaknesses of the current legal framework, calling for an adaptation of the legislation. A reform is currently under development, and after more than two years since its official release it is reaching its final stages. It is expected to be finalized by the end of 2015, thus entering into force in 2017, at the earliest.

The reform is composed of a Directive for judicial cooperation in criminal matters, as well as a widely-applicable General Data Protection Regulation (GDPR). The latter shall replace the current Directive 95/46/EC. The Regulation builds on the principles and rules of the pre-existing Directive, but aims to enhance the rights of the DS. Also, it emphasizes the responsibility of the data controllers and processors and increases the sanctions for violations of its provisions.

The new Regulation will place a significant burden on businesses involved in the processing of personal data. Enterprises will be required to comply with a new regime which is rather vague, building on concepts such as *appropriate measures* or *legitimate purpose*. While enterprises will have a significant interest in being compliant with the GDPR, they are faced with the absence of any concrete guideline or consolidated approach to defining compliance with these requirements. At this point, what is missing is an understanding of the legal and technical challenges in achieving compliance with GDPR requirements. We believe that the academic community needs to discover the overlapping topics where legal requirements meet business practices in cloud service provisioning.

If we can identify gaps between what data protection regulations stipulate and what is it technically achievable in terms of compliance, we can better understand where to direct meaningful research focus.

While taking into account security concerns for IT systems, the current industrial practice needs to consider the ISO/IEC 27000 standard series that provides a framework to handle concepts such as security policy and objectives, risk definitions and assessment, commitment for continuous evaluation and documentation. In particular, the IT community has already widely accepted the ISO/IEC 27001-2005 (and its last revision ISO/IEC 27001-2013), not only as a business competitive advantage, but also a must-have standard certification for enterprises. The ISO/IEC 27001 certification has progressively become a client requirement: for instance, it is required for the PFS (Professionals of the Financial Sector) agreement delivered by CSSF (Commission de Surveillance du Secteur Financier, an agency that monitor the financial sector in Luxembourg), a business requirement in the Luxembourgish financial sector. The IT community is also showing interest to the new ISO/IEC 27018-2014[1], a standard targeting cloud services. Unfortunately, it lacks practices and return of experience. Since December 2008, the Cloud Security Alliance (CSA) gathers cloud practitioners and companies in order to promote the use of best practices for providing security assurance within cloud computing. They also propose training, based on their open certification framework CSA STAR (Security, Trust & Assurance Registry), that leverages the requirements and control points of ISO/IEC 27001. The CSA is also aware of the difficulties that the new Regulation will entail [1]. In its updated report on the survey about the top threats in cloud computing [2], privacy and data protection are not listed, but many of the threats and suggested best practices therein match some of the provisions and duties within the GDPR, such as risk assessment and data integrity.

The idea of the present approach is to analyze the ISO 27001 standard and the Regulation, extracting the main concepts from both texts. We aim to find a mapping of the concepts expressed by each of these documents. Such an analysis can be used as a starting point to define criteria for GDPR compliance.

In the absence of clear rules and constraints, identifying security standards that can be applied to data protection to bridge the gap between the current practices and the future legal requirements can increase the DSs' trust and provide competitive advantages. It can also ease the transition to a new, consolidated approach to personal data protection.

References

[1] Francoise Gilbert. *What the Proposed EU Data Protection Regulation Means for Cloud Users*. Tech. rep. `https://downloads.cloudsecurityalliance.org/initiatives/clic/CLIC-Proposed-EUDataProtection-20120202.pdf`. Retrieved on 2015, February 9. CSA Legal Information Center (CLIC), Feb. 2013.

[1] Information technology – Security techniques – Code of practice for protection of personally identifiable information in public clouds.

[2] Top Threats Working Group. *The Notorious Nine: Cloud Computing Top Threats in 2013*. Tech. rep. `https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf`. Retrieved on 2015, February 9. Cloud Security Alliance, Feb. 2013.