Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection

Paul de Hert [a,b,*], *Vagelis Papakonstantinou* [a], *Irene Kamara* [a]

[a] *Free University of Brussels (VUB-LSTS), Belgium*
[b] *Tilburg University (Tilt), The Netherlands*

Keywords:
Cloud computing
Standardisation
ISO
Personal data
Security
Confidentiality

ABSTRACT

In July 2014 ISO and IEC published a standard relating to public cloud computing and data protection. The standard aims to address the down-sides of cloud computing and the concerns of the cloud clients, mainly the lack of trust and transparency, by developing controls and recommendations for cloud service providers acting as PII processors. At the same time, the standard aims to assist providers to demonstrate transparency and accountability in the handling of data and information in the cloud. This paper looks briefly at the data protection and security challenges of cloud computing. It discusses the provisions and added value of the standard in the context of the European data protection legislation and also looks at the uptake of the standard one year after its publication.

1. Introduction

In July 2014 ISO and IEC published a new standard relating to public cloud computing and data protection. The new ISO/IEC 27018, "*Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*", is a technical standard aimed at helping cloud providers, when acting as data processors, to comply with their legal and contractual obligations as to their processing of personal data and, in this way, to create a control mechanism for their cloud clients.

The standard is published at a very critical period: Cloud computing is appraised as the solution for many companies that seek to reduce their operational costs and administrative burden. Moving certain processing operations to the cloud saves companies from keeping specialised IT staff and infrastructure on their balance sheets. In this context, cloud computing is an emerging information technology field that boosted its business over the past few years and could potentially grow even further: according to the European Commission, the public cloud could generate €250 billion in GDP in 2020, while creating 2.5 million extra jobs in Europe only[1]. It is also important to note that cloud computing is particularly

* *Corresponding author.* Law Science Technology & Society (LSTS), Vrije Universiteit Brussel, Pleinlaan 2, B-1050 Brussels, Belgium.
E-mail addresses: paul.de.hert@vub.ac.be, paul.de.hert@uvt.nl (P. de Hert), vpapakonstantinou@mplegal.gr (V. Papakonstantinou), Irene.Kamara@vub.ac.be (I. Kamara).

[1] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe", COM (2012) 529 final, 27th September 2012.

http://dx.doi.org/10.1016/j.clsr.2015.12.005

beneficial to SMEs, allowing them to enter new markets and to compete with bigger players. [2]

On the other hand, transparency, confidentiality and control are central concerns of potential cloud clients. The cloud business is developed in such a way that its clients often lack the necessary information on, for instance, how information moved to the cloud is processed and safeguarded or what happens to it in case they want to move to another provider or in the event that their provider terminates its operation or changes, unilaterally, its terms of service. Especially in the EU data protection-centric environment, users are aware of data protection and privacy risks posed by cloud computing and are increasingly concerned on its lawfulness. Recent alleged revelations on personal data (images) leakage on iCloud[3] raise the concerns of the average user and may have an impact on the cloud computing industry.

The European Commission acknowledged the importance of standardisation in cloud computing and the potential of cloud computing standards to build confidence in the cloud market. Furthermore, the new Regulation on European standardisation[4] emphasises the increase of competition, the quality enhancement, the provision of information, as well as the compatibility and interoperability that standards can bring to the market. Standardisation bodies are therefore called upon in order to provide solutions with regard to cloud computing practice problems – some of which, however, are inherent to the cloud computing providers' business models.

The new ISO standard constitutes an attempt to, partly, deal with the above situation. It takes into account the EU data protection concerns (as included in the EU Data Protection Directive[5] that is however soon to be replaced[6]) as well as on the privacy principles of another standard (ISO/IEC 29100). The new standard is auditable, in particular in the context of a so called *ISO/IEC 27001 audit*, which means that the cloud provider can be certified for its compliance with the standard by third party independent certification bodies.

This paper looks briefly at the data protection and security challenges of cloud computing, discusses the new standard and its added value and analyses it in the context of the European data protection legislation. The paper also discusses the uptake of the standard one year after its publication. Sections 1 and 2 introduce the International Organisation for Standardisation, international standards and their legal nature and effect. Section 3 provides a brief background on cloud computing, its models and features, while the following section discusses most common cloud computing data protection risks. Section 5 sets the background of the ISO/IEC:27108 and places it in the landscape of other information security ISO standards. Section 6 looks at the intentions of the developers of the new standard and the objectives the standard aims to achieve. Sections 7–10 provide a critical view at the scope and content of the standard in relation to its objectives and the EU data protection framework; the PII (Personally Identifiable Information), the targeted actors, the principles of the new standard and the accountability and certification. Section 11 concludes the paper by assessing the potential impact of the ISO/IEC:27018 on data protection.

2. The ISO and International Standards

ISO stands for "International Organisation for Standardisation". Based in Geneva, ISO was founded in 1946. Today its members come from more than 145 countries. Since its establishment, ISO has published over 19,500 international standards. In essence, its members are national standardisation bodies, creating thus a strong network of standard-makers. ISO develops voluntary international standards, which "*ensure that products and services are reliable and of good quality*". ISO standards are developed for areas where the industry identifies a need for technical specifications and guidance.

The need for standardisation activity in a specific area is communicated to ISO by either the industry itself or, less often, from consumer associations. The work of ISO is organised in subject areas, ranging from services, energy efficiency and climate change to food and health. The technical committees of ISO develop technical standards, which are then made available to the public. In more detail, the process of developing a

[2] In 2012, the European Commission released the Communication '*Unleashing the Potential of Cloud Computing in Europe*', with the aim to speed up the cloud uptake in Europe: European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe", COM (2012) 529 final, 27th September 2012. The Communication and the accompanying Commission Staff Working Document[1] explain the general approach of the EU on cloud computing, identify the barriers, and set the key actions for the European Cloud Computing Strategy. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014SC0214&from=el.

[3] See articles on press: B. Chen, "Apple says it will add new iCloud security measures after celebrity hack", The New York Times, 4th September, 2014 http://bits.blogs.nytimes.com/2014/09/04/apple-says-it-will-add-new-security-measures-after-celebrity-hack/,K. Hill, "What Apple's changing after massive celeb hack", Forbes, 5th September 2014 http://www.forbes.com/sites/kashmirhill/2014/09/05/what-apples-changing-after-massive-celeb-hack/, D. Wakabayashi, "Tim Cook Says Apple to Add Security Alerts for iCloud Users.Apple CEO Denies a Lax Attitude Toward Security Allowed Hackers to Post Nude Photos of Celebrities", The Wall Street Journal, 5th September 2014 http://online.wsj.com/news/article_email/tim-cook-says-apple-to-add-security-alerts-for-icloud-users-1409880977-lMyQjAxMTA0MDAwNDEwNDQyWj.

[4] Regulation (EU) No 1025/2012.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O J L 281.

[6] Presumably, by the EU General Data Protection Regulation (see European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final, 25.01.2012).