BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 1 • N° 2 • NOVEMBER 2014

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

by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara

Abstract

At a time when cloud computing industry is developing rapidly, mainly due to the flexibility and the cost minimization cloud computing offers, ISO and IEC developed a new standard on cloud computing to deal with issues of protection of PII and security of information. The new 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.

The article examines the strengths and weaknesses of the new standard, its added value to the cloud computing landscape and to data protection, as well as its relation to the European Personal Data Protection framework.

Keywords: cloud computing, standardisation, ISO, personal data, security, confidentiality

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html

ISSN N° 2565-9979. This version is for academic use only

Summary

While cloud computing is emerging, transparency, confidentiality and control are key concerns of potential cloud clients. The cloud business is developed in a way that the cloud clients often lack the necessary information on how the information moved to the cloud is safeguarded, processed and what happens in case they want to move to another provider or their provider terminates its operation or changes terms of its policies.

Following the urge from the European Commission, the national Data Protection Authorities and Information Commissioners for developing standards to facilitate protection of personal data, ISO and IEC developed the new standard ISO/IEC 27108. The article looks at the new ISO/IEC 27018 standard on “Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”. The focus is on its intended purpose, main elements and potential impact. The analysis has a European perspective; the European legislation - current and forthcoming- form the basis of the analysis. Also the need for the new standard and its relation to other standards for cloud computing or protection of personal information are examined.

The ISO/IEC 27018 provides guidance for cloud service providers that process Personally Identifiable Information (PII) and offers a set of controls which the Cloud Service Providers need to implement in order to address the specific risks. The standards aims to address the specific risks of public cloud computing, help build confidence in public cloud computing providers and give guidance on what the cloud providers need to achieve in terms of contractual and regulatory obligations.

Seen as a building block for compliance with the national and trans-national legislation, the standard contain elements from the Data Protection Directive 95/46/EC, such as principles for the quality of processing. It also embraces the principle of accountability. The new standard is auditable, the cloud provider can be certified for his compliance with the standard by third- party independent certification bodies. Two of the main challenges the standard has to overcome for the European market and jurisdiction are the differentiation in terminology from the European legal framework, and its limited scope covering only the cloud service providers only acting as cloud processors.

Potential positive impacts in terms of protection of personal data are identified in the field of encouraging the industry to adopt measures in order to comply with the personal data legislation and taking a step forward in creating conditions of transparency between the cloud providers and the cloud clients. The acceptance of the standard and the ability to live up to the expectations of the developers still remains to be seen in practice.

1. Foreword

In July 2014 ISO and IEC published a new standard relating to public cloud computing and data protection. The new ISO/IEC 27018, under the title "*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 specialized 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 beneficial to SMEs, allowing them to enter new markets and to compete with bigger players.

On the other hand, transparency, confidentiality and control are listed as central concerns of potential cloud clients. The cloud business is developed in such a way that often its clients 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[2] raise the concerns of the average user and may have an impact on the cloud computing industry.

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[3] that is however soon to be replaced[4]) as well as on the privacy principles of ISO/IEC 29100. The new standard is auditable, in particular in the context of an ISO/IEC 27001 audit, which means that

[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

[2] 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 .

[3] 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

[4] 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).

the cloud provider can be certified for its compliance with the standard by third party certification bodies. Will it be a well-accepted initiative by the relevant stakeholders, e.g. the cloud industry and its clients as well as regulators, and in this way manage to bring an increased level of transparency and accountability in the field? In particular, will it enhance compliance to the, admittedly strict, EU data protection legal requirements? Or will it follow the fate of other initiatives that started with high expectations and ended in long fruitless discussions[5]? The forecast this time seems to be positive. What is certain is that the issues at stake now are more pressing than ever.

2. International Standards and the ISO

ISO stands for "International Organisation for Standardisation". It is a non-governmental organisation that is based in Geneva and was founded in 1946. Today its members come from more than 145 countries. ISO since its establishment has published over 19500 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 the areas where the industry identifies a need for technical specifications and guidance.

This 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 standard may take up a prolonged period of 24, 36 or even 48 months[6] that involves various stakeholders and may be divided into six stages, starting with the proposal and ending with publication of the end-result[7]. The members of ISO may either participate or observe the procedure. The participating members nominate experts in the technical committees. Worthy of mention is the stage of enquiry[8], where a draft of the standard under development is published and is opened for comments from the ISO members, so that the final draft takes into account as many views, experience on best practices and market needs as possible.

The outcome of the above process is the international standard itself, which, according to ISO, brings benefits both to the industry (by increasing productivity, helping companies access new markets and reducing the costs from errors) and to the consumer (by facilitating worldwide compatibility of technology and increasing the offer of choices).

3. Legal nature and effect of international standards

International standards are in essence consensus agreements entered between its members "*on the specifications and criteria which are to be applied in a consistent way in the manufacture of products,*

[5] See for example the Do Not Track standardization discussion in W3C.

[6] Provision 2.1.6.1. of ISO/IEC Directives (Part 1 -5th edition) sets the following deadlines: 24 months to publication for accelerated standards development track, 36 months to publication for default standards development track and 48 months for the enlarged standards development track.

[7] The stages for developing an ISO standard are 1. The proposal stage 2. The preparatory stage 3. The Committee stage 4. The enquiry 4. The approval and 6. The publication stage. For more information, see:http://www.iso.org/iso/home/standards_development/resources-for-technical-work/support-for-developing-standards.htm

[8] More details on the stage of the enquiry: International Organization for Standardization, "ISO/IEC Directives, Part 1, Consolidated ISO Supplement- Procedures specific to ISO", 5th edition, 2014, http://www.iso.org/sites/directives/directives.html#toc_marker-27

the provision of services and the classification of materials"[9]. From this point of view, there are several definitions of standards. The ISO/IEC definition, as found in EN 45020, refers to a *"document, established by consensus and approved by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits".*[10]

From an EU point of view the 98/34/EC Directive[11] regards the standard as a technical specification[12]. More specifically, according to its Art. 1 (6), a standard is *"a technical specification approved by a recognised standardisation body for repeated or continuous application, with which compliance is not compulsory (..)"* and an international standard is a *"standard adopted by an international standardisation organisation and made available to the public".* The new Regulation 1025/2012 on standardisation[13] slightly improves the above definition, aligning it with actual practice: " *'standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory*".

Standards are -in principle- voluntary. Since there is no requirement for compliance, standards do not have a binding legal status. The same goes for international standards. ISO standards are voluntary, which means that there is no, formal legal, requirement for compliance. Despite this lack of formal legal effect, standards can be regarded as *soft law*, especially the ones that aim at specifying how to fulfil a legal obligation. This is the case with the so-called "*harmonised standards*"[14]. Harmonised standards are drafted on the basis of a request from the European Commission to the European Standardisation Organisations to provide a standard which provides solutions for compliance with a legal provision. They remain voluntary, but their implementation offers the implementing party a presumption of conformity with the specific provision of the legislation addressed by the harmonised standard[15]. The parties which have to comply with a legal obligation are free to choose alternative ways to comply with their obligations, apart from the implementation of the technical standards. Notwithstanding, however, the above, there is no equivalent of "harmonised standards" at international level. International standards remain voluntary sets of regulations that, perhaps under suitable circumstances (for example very broad acceptance by the industry, no regulatory alternatives etc.), could achieve at best the status of *soft law*.

[9] See www.iso.org.

[10] EN 45020: 1993 - General terms and their definitions concerning standardisation and related activities(ISO/IEC Guide 2: 1991), Section 3.2.

[11] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulation, OJ 1998 L 204/1, as amended.

[12] Art. 1 (3) provides the definition of a technical specification: "*a specification contained in a document which lays down the characteristics required of a product such as levels of quality, performance, safety or dimensions, including the requirements applicable to the product as regards the name under which the product is sold, terminology, symbols, testing and test methods, packaging, marking or labeling and conformity assessment procedures"*.

[13] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, OJ 2012 L/316.

[14] Read more on the website of the European Commission: http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/index_en.htm

[15] For *example, in the area of explosives for civil uses, the Directive* 93/15/EEC [Council of the European Communities, Council Directive 93/15/EEC of 5 April 1993 on the harmonization of the provisions relating to the placing on the market and supervision of explosives for civil uses, OJ No L 121 of 15 May 1993] sets the legal framework for placing on the market and supervision of explosives for civil uses. Based on this Directive, there is a list of harmonised standards developed by the ESOs and referenced in the Official Journal of the European Union, relating to specific provisions of the Directive and providing guidance to the industry on the fulfillment of the legal obligation foreseen in those provisions.

In the previous paragraph we examined the legal status of (ISO) standards as such. Despite their relatively low ranking when compared with formal legal requirements, standards may develop binding legal obligations for the parties concerned in the event that they are expressly incorporated into a contractual relationship. Such contractual relationships normally cover business relationships between the same parties[16]: the seller of a product or the provider of a service and the buyer/consumer or recipient of the service. In the event that an (ISO) standard is expressly referred to (or even incorporated in full) in the relevant contracts and is subsequently allegedly infringed, sellers could face claims by their clients on the basis of contractual liability[17] or tort[18].

Consequently, despite their essentially voluntary nature, standards are not necessarily non-binding instruments. Apart from formal legal distinctions, the beliefs and expectations of the parties involved may also prove of legal (and not only of commercial) value. Once a party chooses to apply a standard a presumption of compliance applies, meaning that such party is assumed at all times to comply with the requirements set in the standard, which in turn are expected to be lawful themselves. A multitude of legal consequences may be presumably derived from this statement, such consequences applying in parallel to the formal legal distinctions made above. At any event, however, for the purposes of this analysis it is important to be noted that standards are in principle not directly related to legal obligations, and compliance with a standard does not reduce the burden of the party concerned to conform with the law and take every measure necessary to this end.

4. Cloud computing, personal data protection and standardisation

The European Commission released the Communication '*Unleashing the Potential of Cloud Computing in Europe*'[19] in 2012, with the aim to speed up the cloud uptake in Europe. The Communication and the accompanying Commission Staff Working Document[20] explain the general approach of the EU on cloud computing, identify the barriers, and set the key actions for the European Cloud Computing Strategy.

An already identified cloud computing shortcoming at that time referred to the "*jungle of standards*" [21], causing lack of certainty on, among others, interoperability, protection of personal data and protection against data breaches and cyber-attacks. 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[22] emphasizes 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.

[16] See in particular Stuurman, C. & Wijnands "*Legal Apects of Standardisation in the Member States of the EC and opf EFT"*. Falke, J. & Schepel, H. (eds.). , H. S. A. 2000 , Luxembourg: Office for Official Publications of the European Communities, p.610. However, for the purposes of this analysis *the issue whether the standardisation organisation may be held liable for inadequate stipulations within its own standard is not examined.*

[17] Walden, Ian, and Niamh Christina Gleeson. "'It's a Jungle Out There'? Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law, 23rd May 2014.

[18] Stuurman ibid, p. 605.

[19] 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.

[20] Available at: http://euapm.eu/wp-content/uploads/2013/04/STAFF-WORKING-DOCUMENT-Unleashing-the-Potential-of-Cloud-Computing-in-Europe.pdf

[21] National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing*, Special Publication 800-145, September 2011, p.2.

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

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, as will be immediately demonstrated in the analysis that follows.

4.1 Cloud computing rollout and service models

Cloud computing started as an in-business infrastructure built by major companies such as Microsoft, Google and Amazon for their own business needs. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space[23].

The European Commission provides a function-based description of what cloud computing is; "*the storing, processing and use of data on remotely located computers accessed over the internet*"[24]. The definition includes critical characteristics of cloud computing such as the computing power provided to the users "on demand", the remote access of the data and the facilitating role of the Internet. A more technical definition is given by the National Institute of Standards and Technology (NIST), which defines cloud computing as: *"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".*[25]

According to NIST[26], the "cloud" is composed of five essential characteristics. The first characteristic is the *on-demand self-service*, meaning that the consumer may demand and receive the service without human interaction with the service provider. For instance, in creating a Dropbox account and using cloud storage services, the cloud client does not need to interact with a Dropbox representative to establish the relationship and receive the service. Similarly, after initiation of the service a cloud client has access to it automatically, again without provider intervention. Another characteristic is the *broad network access*, in the sense that services are available over the network and are accessed through standard mechanisms. Other characteristics are the *rapid elasticity* of the cloud capabilities and the fact that it is a *measured service*. The latter means that cloud systems automatically control and optimize the use of their resources. This last characteristic is one of the key success factors of cloud computing, as it *reduces radically the costs of the service*. Last but not least, resource pooling is an essential characteristic of the cloud. The computing resources of the provider may be perceived as a "pool", from which multiple consumers are served. This multi-tenant pool of different physical and virtual resources such as storage, memory and network bandwidth assigns and re-assigns the several resources depending on the demand from the cloud client.

Cloud computing may be distinguished into *private*, *public*, *community* and *hybrid*[27]. The *private* cloud is destined for exclusive use by a single organisation. Its ownership, management and operation however does not necessarily belong to the user; it may belong to another third party and exist on or off premises[28]. The *public* cloud on the other hand is owned by a provider who is specialised

[23] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", wp196, adopted on 1 July 2012.

[24] 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, p. 2

[25] NIST, ibid.

[26] Ibid.

[27] The terms "types", "deployment models" and "rollout models" are used interchangeably in the paper.

[28] NIST, ibid, p.3

in the supply of services that makes available his systems to users, businesses and administrative bodies[29]. Public cloud is provisioned for use by the general public and exists on the premises of the cloud service provider. As the Article 29 Data Protection Working Party emphasises[30], the cloud client is bound to transfer a major portion of its control over the data to the cloud service provider. Consequently, the service provider in the public cloud deployment model plays a key role for the protection of the data transmitted to its systems. The *community* model resembles to private cloud with the difference that it is provisioned not to an organisation, but to a community of consumers from organisations with common interests and concerns. It is owned by one or more organisations within the community or a third party, and exists on or off premises[31]. Finally, the *hybrid* cloud is a combination of two or more cloud types, which keep their integrity but share technology among them, which facilitates data portability.

According to the Article 29 Data Protection Working Party[32] the cloud service models are the Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). A study of the European Parliament in 2012 also adds the storage as a service to these models[33]. The simplest model of cloud is the storage as a service, which allows customers to store and share data remotely[34]. SaaS is the model where the cloud client uses the applications of the provider that run on the cloud infrastructure. This model provides complete remote software environment to the customers for instance for email, word processing, calendar or other similar uses. The offered applications are often meant to replace the applications installed by users in their local computer systems[35]. The PaaS cloud service model enables software developers to build applications on the cloud, benefiting from the underlying cloud infrastructure. The cloud infrastructure is not managed or controlled by the client, who has control only over its applications. The fourth model, IaaS, in terms of client control is more advanced than the other models. The cloud service provider leases a technological infrastructure to the customer. In IaaS, the cloud service provider gives control to the client over the computing and storage resources (i.e. infrastructure) of the cloud. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)[36]. Greater control means higher level of expertise, since it is not possible for the average user to take advantage of this flexibility and control in the IaaS model.

[29] Article 29 Data Protection Working Party, ibid, p.25

[30] Ibid.

[31] NIST, ibid.

[32] Ibid.

[33] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, “Study Cloud Computing”, May 2012, p. 19.

[34] European Parliament, ibid, p. 19.

[35] Article 29 Data Protection Working Party, ibid, p. 26.

[36] NIST, ibid, p. 7.

4.2 Cloud computing data protection risks

An important part of the user concerns, when it comes to cloud computing, refers to personal data protection issues. Cloud service providers process personal data either of the cloud client but also of third parties. As the Article 29 Data Protection Working Party notes[37], the majority of the risks relating to cloud computing fall within the categories of lack of control over the data and absence of transparency. It should also be noted that these specific data protection cloud-related risks are to be met regardless of the actual service model implemented.

Lack of control according to the Article 29 Data Protection Working Party is met when the cloud client (data subject) does not have control over the organizational and technical measures that the cloud service provider deploys in order to ensure availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data.[38] It is reasonable for a cloud client to be concerned by the lack of interoperability and the consequent vendor lock-in, for example. Additionally, it is true that, especially in SaaS cloud computing cases, the cloud client and cloud service provider agreement is only a take-it-or-leave-it arrangement between the two parties. The client lacks the power to negotiate and tailor the contract to its needs and to allocate responsibilities in a fair and reasonable way (e.g. without over-excluding limitation of liability clauses for the cloud service provider). This establishes a contractual asymmetry that adds to the risk of lack of control[39].

Business to business (B2B) cloud computing implementations only add to the complexity, because another layer of actors is inserted in the above scheme. In specific, when cloud service clients are data controllers themselves, such lack of control jeopardizes their ability to comply with their own data protection legal obligations. These obligations are inextricably connected to the exercise of control over the data and the processing operations. When a cloud client acting as data controller cannot warrant the isolation of the data due to its own lack of control over the technical means of its cloud provider, that in this case acts as a processor and might be using multiple tenancies without the appropriate measures for safeguarding that the data provided by different cloud clients remain separate, then that cloud controller might not be able to meet, for instance, its obligations of Art. 17 of the EU Data Protection Directive for security of the personal data. Moreover, such lack of control might render it not possible for the same data controller to comply with the obligations of Art. 12 (right of access, rectification, blocking) and Art. 14 (right to object, erasure) of the same Directive. In the same context, the general principles relating to data quality might be at risk. It is difficult to imagine how a cloud client who is not in control of its own data processing operations would be able to guarantee, for example, that the personal data will not be further processed for purposes incompatible with the ones for which they were originally collected, as Art. 6(1)b and Art. 6(2) of the EU Data Protection Directive require.

With regard to transparency, it should be noted that transparency is a fundamental principle in the personal data protection legislation, enshrined mainly in Art. 10 of the EU Data Protection Directive, which establishes the obligation of data controllers to inform data subjects on their processing activity, the purposes of processing as well as their identity. The principle of transparency is the

[37] Article 29 Data Protection Working Party, ibid.

[38] Ibid.

[39] See also European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe'", 16 November 2012, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

foundation of other provisions as well, such as Art. 12(a) on the obligation of the data controller to confirm to the data subject – without excessive delay or expense – the fact that the data subject's personal data are being processed. Cloud providers should be transparent towards their clients, in order for them to maintain a first level of control through awareness of the processes, means and measures of the cloud provider, and, also, they should be transparent towards their competent supervisory authorities. In cloud computing the risk of infringement of the relevant provisions related to transparency is increased due to the specificities of cloud computing, such as the chain of subcontractors that are involved in the processing of the data. In practice, cloud providers outsource several parts of their business to external parties. These parties, related to cloud client as sub-contractors of the cloud provider, may have access to the personal data and may well process them in the course of their duties and are as a result obliged to comply with the EU Data Protection Directive. In practice, control over all the sub-contractors and every processing operation might be technically and administratively difficult and costly.

Further data protection difficulties stem from the fact that cloud clients do not usually know where their data are stored[40]. The lack of information on the geographic locations of the data as well as the transfers to different countries, as per the providers' business models, pose risks to the protection of personal data that need to be taken into account. The location of the data is usually connected to the applicable law and jurisdiction. The current European data protection framework requires in order to be applicable either establishment of the controller on a territory of a Member State of the EU or the controller making use of equipment situated on EU territory and such use to be for other than mere transit purposes[41]. As long as the EU Data Protection Directive is applicable transfers to third, non-EU countries should fulfill the requirements of its Art. 25 on the transfers of personal data to third countries, thus an adequate level of protection of the personal data needs to be warranted. In practice, data are hosted in several locations, wherever the servers of the cloud provider are located. This might be in different countries or continents, and indeed in such a dynamic way that makes it troublesome for the provider itself to keep an overview of the transfers of the data and consequently to comply with the legislation.

Along with the above risks, erasure of data is also a data protection risk in cloud computing. Data subjects have the right to delete their personal data that do not comply with the provisions of the EU Data Protection Directive, in particular in case of inaccurate or incomplete personal data (Art. 12(b)). According to a report published by ENISA in 2009[42], reuse of hardware resources increases the risk of incomplete and insecure data deletion in the cloud environment.

4.3 EU data protection legislation and standardization

The role of standardisation in personal data protection has been through a phase of maturity. The EU Data Protection Directive, a legal text corresponding to the needs of an era before the emergence of the internet and cloud computing, acknowledges the benefits of self-regulation in Art. 27(3), in the form of a code of conduct. Nevertheless, the text of the proposed General Data Protection Regulation and the relevant European Parliament report[43] that has already been published

[40] Carlin S., Curran K., "Cloud Computing Security", International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011, p. 17.

[41] Art.3 of the EU Data Protection Directive.

[42] ENISA, Catteddu, D. & Hogben, G. (eds.), "Cloud Computing: Benefits, risks and recommendations for information security", November 2009, available at: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[43] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the

explicitly refer to standardisation in data protection, acknowledging in this way the potential contribution of the former to the latter.

The proposed Regulation handles technical standards as an indispensable part of the new legislation. Standards are seen as a means to achieve a desirable technical result, safeguarding the rights of data subjects and facilitating the compliance of the controllers with the data protection legislation. Taking as an example Art. 13a (amendment 109) of the LIBE Report, data controllers benefit from a standardized information policy, because by following the standard, they know how their legal obligation to inform data subjects are translated into practical steps they need to take in order to be compliant. At the same time, data subjects also benefit from the same standards, as they do not have to deal anymore with different kinds of formats, outlays and content in the information policies. Through a standardized information policy data subjects know where to find the information they are looking for and can therefore exercise their rights more efficiently. Moreover, the proposed Regulation makes several references to technical standards and certification schemes in order to warrant, among others, security, technological neutrality, interoperability and innovation (Recital 66), transparency and compliance with the Regulation (Recital 77) as well as trust among data subjects and legal certainty for controllers (Recital 77).

It should also be noted that Member State Data Protection Authorities support the role of standardisation in the protection of personal data. ICO, the British Data Protection Authority, supports standards, which are recognized by the industry, in order to help cloud service customers compare the services of the cloud providers and rely on an independent assessment[44]. Many DPAs have issued relevant statements, encouraging standardisation activities in the field of cloud computing: the 34th International Conference of Data Protection Commissioners recommended to put effort in, among others, certification and standardisation in order to build trust in cloud computing[45].

5. Why the specific need for this new standard?

Given the substantial data protection risks posed by cloud computing measures need to be undertaken in order to mitigate their effect, to the benefit of the cloud computing industry, its clients as well as data subjects (when different from such clients). As explained, the approach of the law towards standardisation in the field of data protection is more than positive. This has triggered various initiatives from the European Commission, non-governmental organisations, the industry itself etc. This new standard therefore is not the first in its field and it certainly will not be the last. The question therefore that comes to mind is what does ISO/IEC 27018 bring to the landscape of privacy-related standards? What is its added value? However, before addressing these questions, it is important to the purposes of this analysis to briefly examine already existing standards that deal with information management, security and privacy. The overview of the other standards is limited to ISO standards only, because it is more efficient to compare and identify the added value of ISO/IEC 27018 when examining the evolution within the same standardisation body.

5.1 Previous ISO privacy-related standards

ISO has been working on information technology standards through its Joint Technical Committee

processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM (2012) 11, 22 November 2013.

[44] ICO, "Guidance on the use of Cloud computing", v.1.1., published 2nd January 2012.

[45] Data Protection and Privacy Commissioners, "Resolution on Cloud Computing"34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26th October 2012.

1 (ISO/IEC JTC1), whose secretariat is operated by ANSI, the US standardisation body. ISO/IEC JTC1 aims at promoting and facilitating international IT standards regarding the design, performance and quality of IT products, security of IT systems and information, interoperability of IT products and tools, and others[46]. The subcommittees of ISO/IEC JTC1 are working on areas such as smart cities, big data, internet of things, cards and personal identification, automatic identification and data capture techniques. More specifically, it is its Subcommittee 27 that is developing standards for the protection of information and ICT, including generic methods, techniques and guidelines to address security and privacy aspects[47].

ISO has already published the ISO/IEC 29100 "*Information – Technology-Security techniques – Privacy framework*". The standard provides a general privacy framework for information and communication technology systems. It establishes common terminology (which is not fully in line with the terminology of the EU ata protection legislation), defines the actors in data processing and describes privacy safeguarding measures.

In terms of information security management, the 27000 series provides control objectives and guidance for the protection of information security management systems (ISMS). The ISO/IEC 27000 standard was issued in 2009 in order to provide a foundation on common concepts[48]. The ISO/IEC 27000 family is based on the principle "Plan-Do-Check-Act", emphasizing the importance of process orientation, integration and constant checking of implementation[49].

Finally, the ISO/IEC 27001 standard, under the title "*Information technology - Security techniques - Information security management systems – Requirements*", lists requirements for the establishment and operation of an ISMS and covers high level operational and staffing issues[50]. In the same context the ISO/IEC 27002, "*Information technology - Security techniques - Code of practice for information security controls*", gives guidance on practices on selection, implementation and management of controls in ISMS. It is designed to be used as a reference for selecting controls within the process of operating an ISMS based on the ISO/IEC 27001. The standard highlights the importance of risk assessment in order to determine appropriate action. Both 27001 and 27002 standards were revised in 2013.

5.2 Background of the new standard and relationship to previous standards

The new standard, under the title "*Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*" is a sector-specific standard. It provides guidance for cloud service providers that process Personally

[46] Read further on ISO/IEC JTC 1 webpage at: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm

[47] ISO/IEC JTC1 SC38 SGCC, "Study Group Report on Cloud Computing", published 23rd September 2011, Annex A.1.2. p. 28, available at: http://isotc.iso.org/livelink/livelink/fetch/-8913189/8913214/8913373/Study_Group_on_Cloud_Computing_final_report.pdf?nodeid=12096352&vernum=-2

[48] ISO/IEC 27001, "Information Technology, Security Techniques, Information Security Management Systems, Requirements," International Organization for Standardization ISO, Geneve, 2005.

[49] Disterer, G., "ISO/IEC 27000,27001 and 27002 for Information Security Management", Journal of Information Security, 2013, 3 pp. 92-100.

[50] Mitchell C., "Standardising privacy and security for the cloud", Royal Holloway, University of London, presentation at presented at STEM-UEN & Microsoft Advanced Technology Workshop: Cloud Computing enabling Innovation, Kingston University, 1st November 2011, available at: http://www.chrismitchell.net/Publications.htm#Seminars

Identifiable Information (PII) and offers a set of controls which the Cloud Service Providers need to implement in order to address specific risks. The rationale behind it was to create a standard that would address the specific risks of public cloud computing and help build confidence in public cloud computing providers while also providing guidance on what cloud providers need to implement in terms of contractual and regulatory obligations[51]. More specifically, the reason for the development of the ISO/IEC 27018 standard lies with the obligation of Art. 17 of the EU Data Protection Directive for the controller to implement technical and organisational measures to safeguard the security of its data. Within the context of this obligation the controller must choose a processor that provides sufficient guarantees in terms of organisational and technical security measures for the processing and ensures compliance with the measures. As explained above, lack of transparency and lack of control over the data are two common cloud privacy risks. The new standard provides the cloud provider, when acting as a data processor in the context of the EU Data Protection Directive, with practical guidance through establishment of concrete procedures and measures while at the same time offering the opportunity to demonstrate their adequate implementation to the controller via a certification scheme, as the standard is auditable by a third independent certification body.

The standard was developed by Working Group 5 within the ISO/IEC JTC1/SC27, which is concerned with Privacy and Identity management. The WG5 started working on a draft in the beginning of 2012; the standard was published in August 2014[52]. The end-result has undergone reviews and consultation with contributors from fourteen (14) countries and five (5) international organisations[53]. The Article 29 Data Protection Working Party made comments on the second working draft of the standard in March 2013.

As mentioned above, the ISO/IEC 27001 provides a system for identifying information security risks as well as control sets to address them. The new ISO/IEC 27018 seems to add to the risks and controls of the 27001 and 27002 more specific ones that are encountered in a public computing environment. When it comes to the relationship between 27002 and 27018, 27002 concerns mainly controls regarding confidentiality, integrity and availability, while the new standard focuses on information privacy risks from the perspective of PII processor[54]. In essence, the new standard builds upon the 27002, something which is clearly stated in the text of the standard itself: "*The international standard has been based on ISO/IEC 27002*"[55] and "*this International Standard augments the ISO/IEC 27002 controls to accommodate the distributed nature of the risk and the existence of a contractual relationship between the cloud service customer and the public cloud PII processor*"[56]. This is done in two ways: first, the ISO/IEC 27018 provides guidance as to how the controls of 27002 can apply to the public cloud service provider acting as a PII processor; and, second, by means of an Annex including additional set of controls. As to its relationship with the ISO/IEC 29100, the new standard uses the privacy framework, principles and vocabulary of the 29100, apparently for reasons of consistency and continuity. Finally, as a general remark, it should be noted the standard is called "*code of practice*". Unlike the ISO/IEC 27001, both 27002 and 27018 standards avoid the use of "*shall*", so that they are more a reference catalogue than concrete obligations for cloud service providers.

The clear distinction of the areas where the new standard can be useful on the one hand and the

[51] Mitchell C., "Outsourcing personal data processing in the cloud", 25th January 2014, available online

[52] Ibid.

[53] See the list of participating members and liaison organisations to the JTC1/SC27 at http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=members

[54] Philips J., "ISO/IEC 27001, 27002 and 27018", presentation, 15th January 2014

[55] ISO/IEC 27018:2014 s.0.2, vi

[56] ISO/IEC 27018:2014 s.0.2. vii

connection with the controls and measures of the previous standards on the other, offer the possibility to first have a sector-specific standard and second benefit from good practices[57] and approaches that are of more generic nature and might not be encountered only in cloud environments but can still be applied to them.

5.3 Intentions and objectives

Taking into account the noted lack of trust by its clients with regard to both the security and privacy aspects of the cloud as well as the urge of the European data protection regulator for standardisation, ISO in cooperation with IEC started developing the standard under discussion. The general idea behind it was that there would be a sector-specific standard which could be audited and certified. Auditing helps cloud clients overcome the transparency issues that are deterrent for moving whole or part of their processing operations to the cloud. When a cloud client is in position to know what type of measures the cloud service provider implements in order to address specific data protection and security risks, its concerns on lack of information and control, as identified by the Article 29 Data Protection Working Party, are eased. At the same time, the certification by a third body (and not self-certification), helps the cloud service provider demonstrate its robust security technical and organisational measures and comprehensive policies.

Originally the standard drafters' intention was that it would cover personal data processing in a public cloud by both controllers and processors – at least this is what was implied by its original title: "*Information technology – Security techniques – Code of practice for data protection controls for public cloud computing services*". However, at a later stage, when the standard under development became more mature, it was renamed to its current version, replacing "data protection" with "Personally Identifiable Information" and narrowing its scope to cloud providers that act as PII processors. Although this change constitutes an important scope limitation, the removal of the word "*controls*" broadened the standard's scope, in the sense that it does not contain only security controls but also high-level principles and normative references to privacy risks. Together with ISO/IEC 27002 they create a common set of security categories and controls.

The objectives of the standard concern both the cloud services provider and the cloud service customers. These objectives are effectively two sides of the same coin, offering the opportunity for compliance with their legal or contractual obligations to each one of them. As illustrated in the text of the ISO/IEC 27018, the standard is a means for the cloud service provider to comply with its contractual or legal obligations when acting as PII processor and to enable it to demonstrate its compliance. At the same time, the standard is a mechanism that facilitates the exercise of "audit and compliance rights" of the cloud computing client.

The standard also has another objective, addressing the pre-contractual concerns of the cloud service customer on the choice of the appropriate provider. As CNIL notes, while entering a contract it is essential for the cloud service customer to compare the contractual conditions proposed by different providers[58]. The elements that a client ought to look for before entering into an agreement should include, among others, legal constraints (eg. location of the data, guarantees of security and confidentiality), practical constraints (eg. availability, reversability) and technical constraints (eg. interoperability). These requirements need to be met by the candidate cloud service provider at a level at least equal to its own. By referring to a standard, a cloud computing client is able both to

[57] Guilloteau S., "Une nouvelle norme de bonnes pratiques poir la protection des donnees personnelles dans le cloud", published on 2nd September 2014, available at: www.orange-business.com

[58] CNIL, "Recommendations for companies planning to use cloud computing services", published 25th June 2012.

select a provider that is well-governed, when it comes to PII processing, and also to verify whether the level of the offered guarantees corresponds to its own.

6. Key elements of ISO/IEC 27018

6.1 PII instead of personal data

As with ISO/IEC 29100, the new ISO/IEC 27018 uses an autonomous set of terminology, differentiating from the EU data protection legislation terms[59]. Instead of "personal data", the standard employs the term "personally identifiable information". Although the term is borrowed from the US, it does not seem to fully match the one used in several US guidance or normative documents[60]. At any event, the term PII is defined in section 3.2. of the text as: *"any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal".* The first editor's note under this definition mentions that "identifiable" is the information when all the reasonable means that can be used either by the "privacy stakeholder who holds the data" or any other third party are taken into account. On the other hand, according to the EU Data Protection Directive, personal data is " *any information relating to an identified or identifiable natural person".*[61] The European Commission proposal for a General Data Protection Regulation suggests that personal data is "*every information relating to a data subject*", while the European Parliament's input on the same matter reinstituted the notions of identification and identifiability[62].

The PII as employed in the new standard and the concept of "*personal data*" of the EU basic data protection legislation cover to an extent the same cases. But the scope of "*personal data*" seems to be wider: it does not concern only information that "can be used" or "linked" to a PII principal/ data subject, but "any information" relating to an identifiable natural person. The EU definition does not relate the decision on whether a piece of information is personal data to its use: the EU definition covers cases where the information is not or might not be – directly/ indirectly – linked to a natural person, but still this information might identify a person. For example, a session cookie, might not be linked to a natural person. It might be linked to a computer device, but not a natural person. However, the same cookie might identify a person, when combined with a social network plug-in (eg. the log-in data). From the definition of PII, it is not clear whether the latter case of personal data is regarded as PII.

The choice of differentiation from the terminology of the EU data protection legislation is apparently deliberate, but in this regard it might have implications when, for example, an EU-based cloud service provider may need to apply the set of controls of the standard to cases that are not covered by its scope, in order to comply with its legal obligations. In other words, cloud service providers and their clients need to bear in mind that the standard does not address all the cases in order

[59] FIDIS, "D19.3 Standardisation report", published 20th April 2009.

[60] See Guide to Protecting the Confidentiality of Personally Identifiable Information, National Institute of Standards and Technology, pp.1-2, also: Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security, p. 6, Report to Congressional Requesters, Protecting Personally Identifiable Information, United States Government Accountability Office, p.1.

[61] See its Article 2.

[62] According to the art. 4 (amendment 98) of the European Parliament Report, ibid: "*personal data means any information relating to an identified or identifiable natural person (data subject). ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person*".

for a data controller to be compliant with the legislation, but it is specifically aimed at the detailed cases it expressly refers to[63]. Practically, it remains to be seen how the parties strike the right balance by separating compliance with the legislation from compliance with the standard.

6.2 Cloud providers as data processors

The ISO/IEC 27018 concerns only the cloud service providers who act as PII processors, i.e. the providers who process PII for and under the instructions of the cloud service client[64]. In the text of the standard, the distribution of roles is clear: the client is regarded as *PII controller* and the cloud service provider is the *PII processor* (broadly following EU Data Protection Directive terminology). Any deviation from this principle, it is out of the scope of the standard.

This approach admittedly grants to the new standard clarity and specificity. Essentially, by choosing not to follow the various business models implemented by cloud providers to-date (or in the future), which is something that in practice could prove impossible, the standards' drafters succeeded in providing concrete guidance to a specific, and potentially clear-cut, situation: under the new standard cloud providers are only conceived as data processors. It is only these cases that are regulated by it. All other business or practical arrangements will have to resort to the general (data protection) provisions that are applicable each time. Despite its boldness, such self-limitation, however, unavoidably develops also a restricting effect. In essence, the new standard deals with only a small part of the cloud issue: It does not cover neither the cases where the provider is controller of the PII, nor the cases where the provider is joint-controller together with its client.

Problems could also be caused due to the at times difficult distinction between the two roles in personal data processing practice. The Article 29 Data Protection Working Party in its opinion on the concept of data controller and data processor, points out that the two main criteria to determine who is data controller are, first, who is responsible for compliance, and, second, who allocates responsibility[65]. The technical committee which worked on the standard inserted a clarification in its text, explaining that the distinction between PII controller and PII processor "*relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives*"[66]. At the same time however, it is acknowledged that there are cases where the public cloud PII processor may need to "*determine the method for processing PII*", which will be consistent with the general instructions of its customer but without the same customer's "*express instructions*"[67]. It also indicates that in that cases, the provider needs to adhere to the privacy (data protection) principles. The International Working Group on Data Protection in Telecommunications (the Berlin Group), suggests that a controller may allow processing of personal data to be performed by a processor but only in accordance with the controller's *explicit* instructions[68]. Furthermore, accord-

[63] The standard does not also make differentiation with regard to the several controls relating to types of PII, such as sensitive information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. It deals with this issue through an editor's note that this is a matter of local jurisdictions. (see section 10.1.1.).

[64] ISO/IEC 27018:2014, see definition of "PII Processor"

[65] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor", wp169, adopted 16th February 2010.

[66] ISO/IEC 27108:2014, Introduction.

[67] See ISO/IEC 27018:2014, Annex A.2.1.

[68] International Working Group on Data Protection in Telecommunications, "Working paper on Cloud Computing – Privacy and data protection issues – Sopot Memorandum", 51st meeting, 23rd-24th April 2012, available online.

ing to the same, processing according to the controller's explicit instructions in cloud computing entails that a provider cannot unilaterally make a decision or arrange the transmission of personal data (and its processing) to unknown cloud data centers even if this is justified, e.g. as a reduction of operating costs, management of peak loads, copying to backup, etc. The EDPS, in its opinion[69], adds an extra criterion refining the thin line between controller and processor, which is based on the suggested definition of the "data controller" in the proposal for a General Data Protection Regulation[70]: the factor of influence on the underlying activities. The argument is that since the cloud provider designs, operates and maintains the IT infrastructure, it therefore determines the organisation and conditions of the processing activity in certain cases, thus in those cases such provider shouldn't be considered only a "data processor". Consequently, it remains to be seen whether the terminology of the new standard will cause problems while allocating responsibilities and accountability among the actors concerned.

6.3 Personal data protection principles

The ISO/IEC 27018 contains a comprehensive set of controls regarding: 1. Information security policies, 2. Organisation of information security 3. Human resource security 4. Asset management 5. Asset control 6. Cryptography 7. Physical and environmental security 8. Operations and communications security 9. System acquisition, development and maintenance 9. Supplier relationships 10. Compliance 11. Information security aspects of business continuity management.

The purpose as mentioned earlier, is that the cloud service provider as PII processor enables the cloud service client, as PII controller, to comply with its legal (data protection) obligations. Moreover, via these controls, the PII processor is able to conform to its own obligations, either legal or contractual. From an overview of the controls and the guidance in the main text of the standard it is clear that they refer mostly to technical and organisational security aspects and less to the basic data protection principles and legal grounds of processing (at least from the EU Data Protection Directive point of view). Controls for privacy principles of the ISO/IEC 29100 are established in its (normative) Annex A. The Annex refers to purpose limitation and specification, accuracy and quality of the data, and others. The ISO/IEC 27018 also sets a control for the provider for the facilitation of the exercise of the data subject rights (PII principal's rights) to access, correct and erase in a timely fashion the PII.

Within the above context, the standard principles to a large extent correspond to the basic principles of the EU Data Protection Directive. Art. 6 of the Directive provides, among others, that any processing must be lawful and fair to the data subjects and that personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected. The data processing purposes need to be explicit and legitimate and must be determined at the time of the collection of the data. Furthermore, the same article requires that the purposes for further processing should be compatible with the original purposes. The purpose limitation principle is also present in the standard, as well as controls which are founded on purpose specification, quality of data and data minimization. Moreover, there are controls which promote transparency in the relationship of the cloud client and the cloud service provider, including the obligation of the latter to inform the former on legally binding requests, its subcontractors and possible locations of storage of the PII. Quite significant is the prohibition of processing of the PII by the provider for marketing and commercial purposes, which is in line with Art.14 of the Directive, establishing the right of the data

[69] European Data Protection Supervisor, ibid.

[70] The definition adds the word "conditions" to the purposes and means, providing a spherical approach to the activities of the data controller.

subject to object to the processing for direct marketing.

At any event it should be noted however that, although the controls and guidance in the standard may be appropriate for applying certain aspects of the principles, these are not the only measures that the cloud provider, even in its capacity as merely data processor, can and should implement. In that sense, the list of measures and controls as included in the standard is not exhaustive, but it is an indication on what type of measures the provider may take in order to help the controller comply with each principle.

6.4 Accountability and certification

According to the principle of accountability as per the proposal for a General Data Protection Regulation, the data controller has to put in place appropriate and effective measures to ensure the compliance with data protection principles and obligations and has to be able to demonstrate to the supervisory authorities that compliance[71]. In the context of cloud computing, IT accountability is made concrete into "the ability to establish what an entity did at a certain point in the past and how"[72]. The LIBE Report on the original proposal for a General Data Protection Regulation provides that the controller needs to adopt policies and implement demonstrable measures both technical and organisational to ensure and be able to demonstrate the compliance with the Regulation[73].

Elements of the principle of accountability are incorporated into the standard, in particular the data breach notification, privacy by design, audits and certifications. In general, the standard may be seen as an instrument that assists the PII processor to comply with the principle of accountability requirements. Key to the demonstration of compliance in the context of the principle of accountability is third party certification. The cloud service provider that implements the new standard may ask for a conformity assessment[74], in order to be certified for complying with the standard. ISO does not undertake certification activities, it has however issued instructions on how to develop an auditable standard. The conformity assessment is performed by certification bodies, which are third parties to the relationship of the client and service provider[75]. The audit and certification is not foreseen to be performed by public authorities. The certification stage within the whole international standardisation system is driven by private companies.

Even though the standard addresses data protection issues and it would possibly make sense for national Data Protection Authorities to be able to audit its implementation, there are three important arguments against such practice: first, the fact that auditors audit and certify the compliance of the companies with the standard and not the law. As it will be later demonstrated, compliance with the standard does not necessarily mean compliance with the (data protection) law. In many cases the standard is only a building block for compliance with legal obligations. The DPAs therefore could audit and certificate the standard only if itself would be formally ratified as being fully compliant with the applicable law. Even in that case, however, in the event of cross-border personal data processing, as is by definition the case in cloud computing, the fact that the standard would mean compliance in full with the law of a single jurisdiction, as certified by the relevant DPA, would not

[71] Article 29 Data Protection Working Party, "Opinion 3/2010 on accountability principle", wp173, adopted on 13 July 2010. Accountability is also one of the principles of the ISO/IEC 29100 standard (see section 5.10).

[72] Article 29 Data Protection Working Party, ibid.

[73] See art. 22 amendment 117 of the European Parliament Report, ibid.

[74] Conformity assessment is the "demonstration that specified requirements relating to product, process, system, person or body are fulfilled": ISO/IEC 17000.

[75] ISO/IEC Guide 65 to ISO/IEC 17065.

necessarily mean that other jurisdictions (and DPAs) would follow. In order to achieve such "automation" an elaborate system of bilateral, cross-country, presumably DPA-led, agreements would have to be entered. While such a scheme would potentially be possible under an EU Regulation regime on data protection, along the lines of the one currently under discussion, third (non EU) countries would probably find it impossible to participate.

Last but not least, if the standard were to be audited by DPAs a "function creep" phenomenon would probably develop, because the same authority issuing a certificate for compliance with the standard would at the same time be responsible to monitor compliance of the same data controller with the data protection legislation within its competences as a national authority established to protect the right of personal data. In such an event, this double functionality of a DPA would most likely raise questions as to its independence as well as impartiality, undermining thus its basic data protection monitoring mission. Admittedly, today, audit functions exist in DPAs; for example the UK ICO monitors the compliance with data protection legislation and at the same time performs audits and advisory visits to organisations which want to improve their processing of personal data. However, the consensual audits and advisory visits of ICO differ substantially from auditing a standard, as the ICO activity resembles more to an assessment of the policies and practices of the organisations in order to assist them comply with the legislation, whereas the audit based on the standard is a third party audit of the processes and measures of the organisation in order to provide (or not) the certificate of compliance.

Consequently, compliance with the standard ought best be audited by private certification bodies. To this end, self-assessment would not be a preferred policy option[76]. The main forms of conformity assessment are testing, certification, inspection, auditing, evaluation and examination. A typical audit process, as per ISO guidelines, is usually divided into specific steps. First, the auditor identifies the sources of information. He or she then collects the information by sampling and verifying and uses the collected information to establish audit evidence. The auditor subsequently evaluates the information and evidence against the audit criteria. As a final stage, before concluding the audit, the auditor identifies the findings of the audit and reviews them[77]. The controls of the ISO/IEC 27018 are audited within the audit of the ISO/IEC 27001 standard on Information Security Management. According to ENISA, which analysed the certification scheme of the previous version of ISO/IEC 27001:2005, continuous monitoring is not part of the framework. However, annual re-certification by a certification body is required[78]. It should also be highlighted, that this minimum framework of controls is fixed, meaning that when controls are not selected by the provider relevant justification and documentation ought to be provided.

Auditability and certification are important features for building trust: the combination of standards with certification by independent parties may enhance trust in cloud services and help controllers and processors achieve compliance with regulatory frameworks[79]. What needs attention though is the way certifications and communicated in the potential cloud client market. Certification on the controls of the new standard demonstrates the compliance of a provider with the standard, in particular under its scope and limitations as discussed above, and should therefore not be advertised as something broader than it actually is.

[76] ENISA, ISO/IEC 27001 Certification, https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes

[77] ISO, UNIDO, "Buidling trust. The conformity assessment toolbox", available on ISO website

[78] See ENISA, ISO/IEC 27001 Certification , as above.

[79] European Data Protection Supervisor, ibid.

7. Potential impact on data protection and other concluding remarks

The new ISO/IEC 27018 standard is the first standard on cloud computing that deals with personal data protection. By developing the standard under discussion ISO and IEC responded in a timely and practical manner to a need of both the market participants, i.e. the industry and the consumers, and (data protection) regulators. As highlighted by practically all EU regulating or monitoring data protection bodies (the European Commission, the European Parliament, the EDPS, the Article 29 Data Protection Working Party), standardisation and certification can play a significant role in the protection of personal data. This policy option is also visible in the text of the EU General Data Protection Regulation currently under discussion: in its text the key role of standardisation is expressly acknowledged in such basic data protection aspects as the fair and lawful processing of personal data, the exercise of the rights of data subjects, data controller and processor accountability etc. As underlined by the Article 29 Data Protection Working Party in its opinion especially on cloud computing, standardisation can mitigate its, important, data protection risks of lack of transparency and lack of control over the data.

Responding to the above needs, ISO and IEC started working on the draft standard. Its explicit purpose was to create an international standard which on the one hand would help the cloud service providers take necessary organisational and technical steps to comply with their obligations while also preserving the supra-national character of an international standard. It is probably exactly this priority, maintaining indeed its international character, that probably explains the careful approach of the standard towards the EU data protection law and requirements. While the new ISO standard tacitly acknowledges the basic EU data protection law (both current, under the Directive, and future, under the Regulation under elaboration) it is extremely careful to draw its distance from it both in terms of scope (providers viewed only as processors) and number of controls included in its text.

With regard to its scope, an important element of the new standard is that it only concerns the cloud service provider when acting as a PII processor. The controls and guidance included in the standard are therefore limited to mainly technical and organisational measures which address exactly this processing case, compliance of a PII processor with its legal obligations. Admittedly, the set of controls, as explicitly mentioned in the standard, may also be applicable for the PII controller, who would however need to take additional measures to comply with its own legal obligations. From an EU data protection law point of view, notwithstanding differences in terminology (that however may be substantial as, for instance, it is not self-evident that a "PII processor" equals a "data processor") and implementation difficulties (a distinction between a data controller and data processor is not always easy), the new standard provides important case-specific guidance to market participants.

The list of controls included in the new standard is also revealing. While a number of basic (EU) data protection principles and obligations are explicitly addressed, the list is expressly not intended to be exhaustive. If compliance with EU data protection law is intended by a PII processor, it will unavoidably have to go beyond what is only written in the new ISO standard. Cloud clients would also presumably need to perform a Privacy Impact Assessment in order to better identify and mitigate data protection risks[80].

[80] De Hert P., Wright D., (eds.), "Privacy Impact Assessment", Springer, 2012.

Such self-limitation on behalf of the new ISO standard drafters was perhaps a wise policy option. Under the contemporary global data protection environment, mostly fragmented and largely divided into the EU and third countries' approach, a uniform, one-size-fit-all[81] ISO standard would probably be either impossible to develop or, if indeed released, of limited practical value. An international standard sets minimum criteria and requirements for complying with obligations stemming either from the legislation or the contract or both. Given the diversity of approaches and legal instruments when it comes to protection of personal data and privacy across the globe it could be said that the expectation for an harmonized standard that would cover and respond to every legal requirement anywhere in the world would be unrealistic. This diversity is frequently met also within otherwise single jurisdictions (for instance, federal and state law in the USA) or seemingly uniform "blocks" of jurisdictions (see, for instance, the lack of uniformity within the EU that led to a draft Regulation in the first place). However, such country fragmentation is incompatible with cloud computing needs and characteristics. Cloud computing is by definition cross-border. Rather than hitting this wall of high expectations and practical limitations, the new ISO standard rationally chose to self-limit its scope into fields it can both realistically cover and offer added-value to its addressees.

The ISO/IEC 27018 does not claim to replace the (data protection) law. It emphasizes that its role is to assist compliance by providing a common framework for providers across the globe. In this way, at least from the EU data protection law perspective, it resembles more to a code of conduct of Art. 27 of the EU Data Protection Directive rather than substitute legislation. This by no way means that the standard is of no practical value; quite the opposite is true. By providing concrete, detailed guidance to a particular, well-defined type of personal data processing, the standard constitutes a building block for compliance with the law. In essence, it provides a framework of controls that can be used to measure and demonstrate compliance with basic EU data protection legislation. Potential participants in the ISO/IEC 27018 process ought therefore keep the above in mind. They would also need to pay attention to certain other characteristics of the same standard. First, they will need to properly place it within its environment: ISO/IEC 27018 is not a stand-alone standard; it builds on earlier ISO standards related to privacy and security by adapting and specifying the controls and guidance for the case of cloud computing. As a result, the standard uses the terminology of the ISO/IEC 29100 and expands the controls of the ISO/IEC 27002:2013 and ISO/IEC:27001. Another basic feature of the standard is its auditability. Compliance with it can be certified by third independent certification bodies performing audits to the activities and processes of the companies adopting the standard. The end result would come in the form of a certificate, demonstrating to potential and current clients as well as to data protection authorities that the cloud service provider (while acting as a processor) takes specific measures for the protection and security of personal information processed in the cloud. Implementation of the standard demonstrates, if not full compliance with the (EU data protection) law, willingness to comply and readiness to treat security and data protection matters in a serious and comprehensive manner.

It is exactly from this point of view that the new ISO standard would probably develop a positive impact even within strict data protection legal environments. Its detailed set of controls and its auditability constitute concrete steps towards compliance and accountability. Its intended use in the market, granting a competitive edge to certified providers, provides concrete incentives to implement – to the benefit of the broader data protection purposes. In this case implementation of data protection-related controls is rewarded, something that might constitute a more interesting approach to providers than what is in place today (penalization in case of breach, if identified by

[81] Bennett. C., "An International Standard for Privacy Protection: Objections to the Objections", Jurisdiction II: Global Networks/ Local Rules, 11th-12th September 2000.

a competent data protection authority). In addition, perhaps most importantly to the cloud industry purposes, the new ISO standard helps build trust between cloud providers, clients and data subjects[82]. Last but not least, the new standard could facilitate, by way of streamlining within its subject-matter, supervision and control by the, already overstretched within their ever-expanding duties, competent data protection authorities[83]. Although the standard is not (and should not be) audited by DPAs themselves, it obliges providers to adopt structured measures and processes for managing specific data protection risks. In the context of an inspection, such structured measures are easier to be tested for compliance with the law than fragmented piecemeal approaches adopted by each provider individually. The new ISO standard could in this way serve as a common point of reference for DPA work across the EU. All the above point to important potential contributions of the new ISO standard to the data protection purposes – a tribute to its self-restricted and rational approach towards its vast and constantly developing subject-matter. It therefore remains to be seen whether implementation in practice will indeed permit it to fully develop its potential and serve its intended purposes.

Literature and sources

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, OJ 2012 L/316

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulation, OJ 1998 L 204/1, as amended

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

Council of the European Communities, Council Directive 93/15/EEC of 5 April 1993 on the harmonization of the provisions relating to the placing on the market and supervision of explosives for civil uses, OJ No L 121 of 15 May 1993

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-(General Data Protection Regulation), COM (2012) 11 final

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Report on the 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 (General Data Protection Regulation)", COM (2012) 11, 22nd November 2013

European Parliament, Committee on Internal Market and Consumer Protection, "Report on the future of the European Standardisation", (2010/2051(INI)), adopted 19th June 2010

European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, "Study Cloud Computing", May 2012

-

Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", wp196, adopted 1st July 2012

[82] Article 29 Data Protection Working Party, ibid.

[83] European Data Protection Supervisor, ibid.

Article 29 Data Protection Working Party, “Opinion 1/2010 on the concepts of “controller” and “processor”, wp169, adopted 16th February 2010

Article 29 Data Protection Working Party, “Opinion 3/2010 on accountability principle”, wp173, adopted on 13 July 2010

CNIL, “Recommendations for companies planning to use cloud computing services”, published 25th June 2012

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

European Commission, DG Information Society and Media, Jeffery, K. & Neidecker-Lutz, B. (eds),”The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010”, 2010, p p. 9-11.

European Data Protection Supervisor, “Opinion of the European Data Protection Supervisor on the Commission’s Communication on ‘Unleashing the potential of Cloud Computing in Europe’”,16 November 2012

ENISA, Catteddu, D. & Hogben, G. (eds.), “Cloud Computing: Benefits, risks and recommendations for information security”, November 2009

ICO, “Guidance on the use of Cloud computing”, v.1.1., published 2nd January 2012

Data Protection and Privacy Commissioners, “Resolution on Cloud Computing”34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26th October 2012

International Working Group on Data Protection in Telecommunications, “Working paper on Cloud Computing – Privacy and data protection issues – Sopot Memorandum”, 51st meeting, 23rd-24th April 2012

-

EN 45020: 1993 - General terms and their definitions concerning standardisation and related activities (ISO/IEC Guide 2: 1991)

ISO/IEC 27018:2014, with the title “Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”, International Organization for Standardization ISO, Geneve, 2014

ISO 27001:2013, “Information Technology, Security Techniques, Information Security Management Systems, Requirements,” International Organization for Standardization ISO, Geneve, 2013.

ISO/IEC 27002:2013, “Information technology - Security techniques - Code of practice for information security controls”, International Organization for Standardization ISO, Geneve, 2013

ISO/IEC 29100:2011 “Information – Technology-Security techniques – Privacy framework”, International Organization for Standardization ISO, Geneve, 2011

ISO/IEC 17000:2004 :”Conformity assessment – Vocabulary and general principles”, International Organization for Standardization ISO, Geneve, 2004

ISO/IEC Guide 65 to ISO/IEC 17065

ISO/IEC JTC1 SC38 SGCC, "Study Group Report on Cloud Computing", published 23rd September 2011

ISO, UNIDO, "Buidling trust. The conformity assessment toolbox"

-

Benett. C., "An International Standard for Privacy Protection: Objections to the Objections",-Jurisdiction II: Global Networks/ Local Rules, 11th-12th September 2000

Carlin S., Curran K., "Cloud Computing Security", International Journal of Ambient Computing and Intelligence, 3(1), 14-19, January-March 2011

De Hert P., "From the principle of accountability to system responsibility key concepts in data protection law and human rights law discussions",

Disterer, G., "ISO/IEC 27000,27001 and 27002 for Information Security Management", Journal of Information Security, 2013

Guilloteau S., "Une nouvelle norme de bonnes pratiques poir la protection des donnees personnelles dans le cloud", published on 2nd September 2014

Mitchell C., "Standardising privacy and security for the cloud", Royal Holloway, University of London, presentation at presented at STEM-UEN & Microsoft Advanced Technology Workshop: Cloud Computing enabling Innovation, Kingston University, 1st November 2011

Mitchell C., "Outsourcing personal data processing in the cloud", 25th January 2014

FIDIS, "D19.3 Standardisation report", published 20th April 2009

National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing*, Special Publication 800-145, September 2011

Philips J., "ISO/IEC 27001, 27002 and 27018", presentation, 15th January 2014

Schallaböck J., "Identity Management and Privacy Technologies", presentation in 9th ETSI Security Workshop, 15th January 2014

Stuurman, C. & Wijnands "Legal Apects of Standardisation in the Member States of the EC and opf EFT". Falke, J. & Schepel, H. (eds.). , H. S. A. 2000 , Luxembourg: Office for Official Publications of the European Communities

Walden, I., and Niamh C.Gleeson. "'It's a Jungle Out There'? Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law, 23rd May 2014

Wright, D. and De Hert P., (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012

-

Chen, B., "Apple says it will add new iCloud security measures after celebrity hack", The New York Times, 4th September, 2014

Hill, K., "What Apple's changing after massive celeb hack", Forbes, 5th September 2014

Wakabayashi, D., "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

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: paul.de.hert@vub.ac.be

N°1 **“The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area”** by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 **“The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection”** by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

BRUSSELS
PRIVACY
HUB
Vrije Universiteit Brussel