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).

standard may take up a prolonged period of 24, 36 or even 48 months[7] that involves various stakeholders and may be divided into six stages, starting with the proposal and ending with publication of the end-result.[8] 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, 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. [9]

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 error) and to the consumer by facilitating worldwide compatibility of technology and increasing the offer of choices.

3. Legal nature and effect of international standards

There are several definitions of standards. ISO defines standards as 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 slightly amends the above definition, aligning it with the actual practice of "*adoption*" of standards by national standardisation bodies instead of a procedure of *approval*, which would entail assessment of the content of the standard before the approval: "'*standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory*".[13] The EU legislation on standardisation reserves a place for international consensus-based specifications. The conditions are the adoption by the European Standardisation Organisations and the generally applicable principle that they do not override the EU law. Importantly, repetition of the EU law text does not have to be part of the standard. The specification which is based on consensus of the parties of the standard development process is enough for the acceptance in the EU jurisdiction.

International standards are in essence agreements between the members of standardisation bodies "*on the specifications and criteria which are to be applied in a consistent way in the manufacture of products, the provision of services and the classification of materials*".[14] Standards are – in principle – voluntary. Since there is no requirement for compliance, standards do not have a binding legal status.[15] The same goes for international standards such as the ones defined by the ISO. 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.[16] This is the case with the so-called "*harmonised standards*".[17] Harmonised standards are drafted on the basis of a request from the European Commission to the European Standardisation Organisations to provide a standard that provides solutions for compliance with a legal provision. Standards remain voluntary, but their implementation offers the implementing party a presumption of conformity with the specific provision of the legislation addressed by the

[7] 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.

[8] 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.

[9] 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.

[10] EN 45020:2009 Standardization and related activities – General vocabulary (ISO/IEC Guide 2:2004), http://www.nbn.be/en/catalogue/standard/nbn-en-45020-1.

[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 labelling 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] See website of ISO: www.iso.org.

[15] P. Hatto, "Standards and Standardisation. A practical guide for researchers", European Commission, DG Industrial Technologies, 2013, p.8.

[16] Guzman and Meyer discussing the concept of "soft law" and the challenges towards a definition of soft law, refer to soft law as "*legally nonbinding commitments from which legal consequences flow*"(Guzman & Meyer, 2010). Gold approaches soft law in international law as expressing a *preference*, instead of not an obligation that a state should act or refrain from acting in a specified manner (Gold 1993).

[17] Read further on the harmonised standards: http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/index_en.htm.

harmonised standard.[18] 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, 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 the status of *soft law*.

In the previous paragraph we briefly 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:[19] 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[20] or tort.[21]

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: history, models and features

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.[22]

In a document by the European Commission it is defined functionally as "*the storing, processing and use of data on remotely located computers accessed over the internet*".[23] 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*".[24]

According to NIST, 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.[25] 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 optimise 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.

[18] 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 harmonisation 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 fulfilment of the legal obligation foreseen in those provisions.

[19] See in particular Stuurman, C. & H. Wijnands "*Legal Aspects of Standardisation in the Member States of the EC and of 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*.

[20] 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.

[21] Stuurman, 2000 ibid, p. 605.

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

[23] 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.

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

[25] NIST, Ibid.

Cloud computing may be distinguished into *private*, *public*, *community* and *hybrid*.[26] The *private* cloud is destined for exclusive use by a single organisation. Its ownership, management and operation however do not necessarily belong to the user; it may belong to another third party and exist on or off premises.[27] The *public* cloud on the other hand is owned by a provider who is specialised in the supply of services that makes available his systems to users, businesses and administrative bodies.[28] 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[29] 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.[30] 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 the cloud service models are the Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).[31] A study of the European Parliament in 2012 also adds the storage as a service to these models.[32] The simplest model of cloud is the storage as a service, which allows customers to store and share data remotely.[33] 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.[34] 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).[35] 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.

5. Most common cloud computing data protection risks

When it comes to cloud computing, an important part of the cloud client concerns relates to personal data protection issues. Cloud service providers process personal data either of the cloud client but also of third parties. The Article 29 Data Protection Working Party notes, the majority of the risks relating to cloud computing fall within the categories of lack of control over the data and absence of transparency.[36] The specific data protection cloud risks exist regardless of the actual cloud service model implemented.

Lack of control according to the Article 29 Data Protection Working Party is met when the cloud client (when acting as data subject) does not have control over the organisational and technical measures that the cloud service provider deploys in order to ensure availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data.[37] It is reasonable for a cloud client to be concerned by the lack of interoperability and the consequent vendor lock-in, for example. Additionally, 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 often 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.[38]

Business to business (B2B) cloud computing implementations only add to the complexity, because another layer of actors is inserted to the above scheme. When cloud service clients are data controllers themselves, such lack of control jeopardises 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

[26] The terms "types", "deployment models" and "rollout models" are used interchangeably in the paper.
[27] NIST, 2000, p.3.
[28] Article 29 Data Protection Working Party, 05/2012, p.25.
[29] Article 29 Data Protection Working Party, 05/2012.
[30] NIST, 2000.
[31] Ibid.
[32] European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, "Study Cloud Computing", May 2012, p. 19.
[33] European Parliament, ibid, p. 19.
[34] Article 29 Data Protection Working Party, 2012, p. 26.
[35] NIST, 2000, p. 7.
[36] Article 29 Data Protection Working Party, 2012.
[37] Article 29 Data Protection Working Party, 2012.
[38] 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.

data controller cannot warrant the isolation of the data due to its own lack of control over the technical means of its cloud provider, then this cloud client might not be able to comply, for instance, with the obligations of Art. 17 of the EU Data Protection Directive relating to the 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. The article 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 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 sub-contract several parts of their business to other cloud companies.[39] 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. 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 the 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 relates its applicability to either establishment of the controller on a territory of a Member State of the EU or the use of equipment situated on EU territory by the controller.[41] As long as the EU Data Protection Directive is applicable, transfers to third non-EU countries should fulfil 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, reuse of hardware resources increases the risk of incomplete and insecure data deletion in the cloud environment. [42]

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 cloud 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?

6. Background of the new standard and relationship to previous standards

ISO has been working on information technology standards through its Joint Technical Committee 1 (ISO/IEC JTC1), whose secretariat is operated by ANSI, the US standardisation body. ISO/IEC JTC1 aims at promoting and facilitating international

[39] Cunningham A., Reed C., "Caveat Consumer? – Consumer Protection and Cloud computing Part 2- The application of ex ante and ex-post Consumer Protection Law in the Cloud", Queen Mary School of Law Legal Studies Research Paper No. 133/2013, February 2013, p. 5.

[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.

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.[43]

The new ISO/IEC 27018 standard, "*Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*" 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 and was published in August 2014.[44] The end-result has undergone reviews and consultation with contributors from fourteen (14) countries and five (5) international organisations.[45] The Article 29 Data Protection Working Party made comments on the second working draft of the standard in March 2013.

ISO/IEC 27018 is a sector-specific standard. It 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 specific risks. The rationale was to create a standard that would address the specific risks of public cloud computing by providing guidance to cloud providers and help build confidence in public cloud computing providers.[46] 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 ISO/IEC 27018 builds on two older standards: the ISO/IEC 27001 and the ISO/IEC 27002.[47] The older standards are information security management standards. The ISO/IEC 27001 provides a system for identifying information security risks as well as controls to address them.[48] The ISO/IEC 27002 includes mainly controls regarding confidentiality, integrity and availability of information systems.[49] The new ISO/IEC 27018 standard focuses on information privacy risks on the public cloud from the perspective of PII processor. In essence, the new standard builds on the ISO/IEC 27002 by adding the elements of "pubic cloud" and privacy, which is explicitly stated in the text of the standard: "The international standard has been based on ISO/IEC 27002" 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". There is a clear distinction of the areas where the new standard can be useful on the one hand and the connection with the controls and measures of the previous standards on the other. This offers the possibility to have a sector-specific standard and benefit from good practices and approaches that are of more generic nature and might not be encountered only in cloud environments but can still be applied to them.[50]

[43] 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: ISO/IEC JTC1 SC38 SGCC, "Study Group Report on Cloud Computing", published 23rd September 2011, Annex A.1.2. p. 28.

[44] ISO/IEC JTC1 SC38 SGCC, Ibid.

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

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

[47] In terms of information security management, the ISO 27000 series provides control objectives and guidance for the protection of information security management systems (ISMS). The ISO/IEC 27000 family is based on the principle "Plan-Do-Check-Act", emphasising the importance of process orientation, integration and constant checking of implementation. : 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. ISO has also 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 data protection legislation), defines the actors in data processing and describes privacy safeguarding measures.

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

[49] 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 ISO/IEC 27001 and ISO/IEC 27002 standards were revised in 2013.

[50] 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.

7. Intentions and objectives of ISO/IEC 27018

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.[51] 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 (instead of a self-certification system), helps the cloud service provider demonstrate its robust security technical and organisational measures and comprehensive policies through an audit by an independent body.

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. The Data Protection Code of Conduct for Cloud Service Providers, published by the C-SIG sub-group on the Data Protection Code of conduct, already includes the ISO/IEC 27018 as a recommended method to achieve the security objectives of the Code of Conduct in terms of privacy risks.[52] 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 aims to address the pre-contractual concerns of the cloud service customer regarding the choice of the appropriate provider. As CNIL notes, while entering a contract is essential for the cloud service customer to compare the contractual conditions proposed by different providers.[53] The elements that a client ought to look for before entering into an agreement should include, among others, legal constraints (e.g. location of the data, guarantees of security and confidentiality), practical constraints (e.g. availability, reversibility) and technical constraints (e.g. 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 facilitated at selecting a provider that is well-governed, when it comes to PII processing, and verifying whether the level of the offered guarantees corresponds to its own. The cloud client is provided with a degree of assurance in meeting its legal data protection responsibilities.[54]

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*

[51] The proposed General Data Protection Regulation, the relevant European Parliament report and the draft of the Council of the European Union explicitly refer to standardisation and certification 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 standardised information policy, as by following the standard, they know how their legal obligation to inform data subjects is translated into practical steps towards compliance. 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 standardised 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): 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, 22 November 2013;Council of the European Union, 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) Preparation of a general approach, 9565./15, 11 June 2015; Also Member State Data Protection Authorities support the role of standardisation in the protection of personal data, such as ICO, the UK Data Protection Authority: ICO, "Guidance on the use of Cloud computing", v.1.1., published 2nd January 2012. 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: Data Protection and Privacy Commissioners, "Resolution on Cloud Computing"34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26th October 2012.

[52] C-SIG sub-group on the Data Protection Code of conduct, "Data Protection Code of Conduct for Cloud Service Providers", no date, p. 30. The Code of conduct, drawn up by the Cloud Select Industry Group (C-SIG) and facilitated by the European Commission, is currently being finalised following the opinion of the Art 29 Working Party. Read further https://ec.europa.eu/digital-agenda/en/news/data-protection-code-conduct-cloud-service-providers. In its opinion on the Code of conduct, the Art. 29 Working Party advised to ideally use the ISO/IEC 27018 "only after assessing the risks on the privacy of the persons concerned, in order to treat them in a proportionate way". Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", WP232, 22nd September 2015, p. 11.

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

[54] Kemp Richard, ISO 27018 and personal information in the cloud: a first year scoreboard, Computer Law and Security Review 31, 2015, p. 554.

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 is 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.

8. The scope of ISO/IEC 27018: "Personally Identifiable Information" (PII)

As with ISO/IEC 29100, the new ISO/IEC 27018 uses an autonomous set of terminology, differentiating from the EU data protection legislation terms.[55] Instead of "personal data", the term of the Data Protection Directive and the forthcoming General Data Protection Regulation, the standard employs the term "personally identifiable information".[56] 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.[57] 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 are "*any information relating to an identified or identifiable natural person*".[58] The European Commission proposal for a General Data Protection Regulation suggests that personal data are "*every information relating to a data subject*", while the European Parliament's input on the same matter reinstituted the notions of identification and identifiability.[59] 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 (e.g. 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.[60] Such cases include different types of personal data, sectors that are regulated by a *lex specialis* such as the financial sector and the cross-jurisdiction differences in the data protection/privacy legislation.[61] 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 for a data controller to be compliant with the legislation, but it is specifically aimed at the detailed cases it expressly refers to. Practically, it remains to be seen how the parties strike the right balance by separating compliance with the legislation from compliance with the standard.

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

[56] Art. 2 (a) of Data Protection Directive 95/46/EC reads: "'*personal data' shall mean 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 identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". According to the EC proposal (2012) for a General Data Protection Regulation, "'*personal data' means any information relating to a data subject*" (art. 4 (2)).

[57] 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.

[58] See its Article 2.

[59] 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*". On identifiability, pseudonymisation techniques and anonymisation read Hon Kuan W. et. al., "The problem of personal data in cloud computing: what information is regulated? – the cloud of unknowing", International Data Privacy Law, 2011, Vol. 1, No.4.

[60] The standard does not 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).

[61] Gleeson and Walden note that "the standard cannot claim to address all the specific differences in every data protection law worldwide" in Gleeson N. and Walden I., "'It's a jungle out there'?: Cloud computing, standards and the law", in European Journal of Law and Technology, Vol 5, No 2, 2014.

9. The targeted actors of ISO/IEC 27018: 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.[62] 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 provide guidance only when cloud providers act as data processors. 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 arise due to the 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 the data controller, first, who is responsible for compliance, and, second, who allocates responsibility.[63] 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*".[64] 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*".[65] In those 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.[66] Furthermore, the Working Group continues that 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 centres 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,[67] 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:[68] 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 should not be considered only as a "data processor". Consequently, it remains to be seen whether the terminology of the new standard will bring obstacles in the allocation of responsibilities among the actors concerned.

10. The principles of ISO/IEC 27018

The ISO/IEC 27018 contains a comprehensive set of controls regarding information security policies, organisation of information security including asset management, asset control and cryptography. Controls of the standard also address human resource security, physical and environmental security, operations and communications security. The standard additionally looks into system acquisition, development and maintenance supplier relationships. Finally, there are clauses on compliance and 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. 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

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

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

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

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

[66] 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.

[67] European Data Protection Supervisor, ibid.

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

on purpose specification, quality of data and data minimisation. 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 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 sole 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.

11. Provisions on 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 compliance.[69] 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".[70] The LIBE Report on the 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.[71]

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, in order to be certified for complying with the standard.[72] 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.[73] 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 entities.

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 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 standards 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 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.[74] The main forms of conformity assessment are testing, certification, inspection, auditing, evaluation and examination. A typical audit

[69] 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).

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

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

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

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

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

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.[75] 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.[76] 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.[77]

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.[78] 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.

12. 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 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 that 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.

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.[79]

Such self-limitation on behalf of the new ISO standard drafters is a deliberate policy option. Under the contemporary global data protection environment, mostly fragmented and largely divided into the EU and third countries' approach, as also epitomised in the recent CJEU *Schrems* decision,[80] a uniform, one-size-fit-all ISO standard would probably be either impossible to develop or, if indeed released, of limited practical value.[81] 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

[75] ISO, UNIDO, "Building trust. The conformity assessment toolbox", available on ISO website.

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

[77] Microsoft and later Dropbox were certified with the new cloud standard.

[78] European Data Protection Supervisor, 2012, ibid.

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

[80] Court of Justice of the European Union, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015.

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

said that the expectation for a harmonised 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 emphasises 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. The added value of the ISO standard is in its potential to provide concrete detailed guidance. The standard constitutes a building block for compliance with the law. Adoption of the standard provides concrete evidence of data protection awareness and willingness to adhere to its requirements – a valuable indicator in the post-Schrems EU data protection environment, where each Member State DPAs is practically authorised to evaluate on its own international personal data transfers[82] that are after all executed not only through social networking websites but also through cloud computing implementations. In essence, the ISO standard provides a framework of controls that can be used to measure and demonstrate compliance with basic EU data protection legislation.

Parties that decide to comply with the ISO/IEC 27018 standard ought therefore keep the above in mind. They would also need to pay attention to certain other characteristics of the 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 is 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 (penalisation in case of breach, if identified by 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.[83] 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.[84] 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 points to important potential contributions of the new ISO standard to the data protection purposes. It therefore remains to be seen whether implementation in practice will indeed permit it to fully develop its potential and serve its intended purposes.

BIBLIOGRAPHY

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 13th July 2010.

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

Article 29 Data Protection Working Party, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, wp232, adopted 22nd September 2015.

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

C-SIG sub-group on the Data Protection Code of conduct, Data Protection Code of Conduct for Cloud Service Providers, no date.

Carlin S, Curran K. Cloud Computing Security. *Int J Ambient Comput Intell* 2011;3(1):38–46.

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

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

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.

[82] See par. 53 of Case C-362/14, ibid.

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

[84] European Data Protection Supervisor, 2011.

Council of the European Union, 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) Preparation of a general approach, 9565/15, 11 June 2015.
Cunningham A, Reed C. Caveat Consumer? – Consumer Protection and Cloud computing Part 2- The application of ex ante and ex-post Consumer Protection Law in the Cloud, Queen Mary School of Law Legal Studies Research Paper No. 133/2013, February 2013.
Data Protection and Privacy Commissioners, Resolution on Cloud Computing, 34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26th October 2012.
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. *J Inform Secur* 2013.
EN 45020:2009 Standardization and related activities – General vocabulary (ISO/IEC Guide 2:2004), <http://www.nbn.be/en/catalogue/standard/nbn-en-45020-1>.
ENISA, Catteddu D, Hogben G (editors.), Cloud Computing: Benefits, risks and recommendations for information security, November 2009.
European Commission. DG information society and media. In: Jeffery K, Neidecker-Lutz B, editors. *The future of cloud computing: opportunities for European cloud computing beyond 2010*. 2010. p. 9–11.
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, 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 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.
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, 22 November 2013.
European Parliament, Committee on Internal Market and Consumer Protection, Report on the future of the European Standardisation, (2010/2051(INI)), adopted 19 June 2010.
European Parliament and Council, 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, OJ L 281.
European Parliament and Council, 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.
European Parliament and Council, Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, OJ 2012 L/316.
European Parliament, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Study Cloud Computing, May 2012.
FIDIS, D19.3 Standardisation report, published 20th April 2009.
Gleeson N, Walden I. 'It's a jungle out there'?: cloud computing, standards and the law. *Eur J Law Technol* 2014;5(2).
Guilloteau S. Une nouvelle norme de bonnes pratiques poir la protection des donnees personnelles dans le cloud, published on 2nd September 2014.
Hatto P. Standards and Standardisation. A practical guide for researchers, European Commission, DG Industrial Technologies, 2013.
Hill K. What Apple's changing after massive celeb hack, Forbes, 5th September 2014.
Hon Kuan W, Millard C, Walden I. The problem of personal data in cloud computing: what information is regulated? – the cloud of unknowing. *Int Data Privacy Law* 2011;1(4).
ICO, Guidance on the use of Cloud computing, v.1.1., published 2nd January 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.
ISO, UNIDO, Building trust. The conformity assessment toolbox.
ISO 27001:2013, Information Technology, Security Techniques, Information Security Management Systems, Requirements, International Organization for Standardization ISO, Geneve, 2013.
ISO/IEC 17000:2004, Conformity assessment – Vocabulary and general principles, International Organization for Standardization ISO, Genève, 2004.
ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls, International Organization for Standardization ISO, Genève, 2013.
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/IEC 29100:2011, Information – Technology-Security techniques – Privacy framework, International Organization for Standardization ISO, Genève, 2011.
ISO/IEC Guide 65 to ISO/IEC 17065.
ISO/IEC JTC1 SC38 SGCC, Study Group Report on Cloud Computing, published 23rd September 2011.
Kemp R. ISO 27018 and personal information in the cloud: a first year scoreboard. *Comput Law Secur Rev* 2015;31:553–5.
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.
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 H. *Legal Aspects of Standardisation in the Member States of the EC and of EFT*. Falke J, Schepel H, editors. H. S. A. 2000, Luxembourg: Office for Official Publications of the European Communities.

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.

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

Wright D, De Hert P, editors. *Privacy impact assessment*. Dordrecht: Springer; 2012.