Personal data and cloud computing, the "cloud" now has a standard

by Luca Bolognini

Lawyer, President of the Italian Institute for Privacy and Data Valorization, founding partner ICT Legal Consulting

Last August the International Organization for Standardization, ISO, published **ISO 27018**, a standard developed specifically for providers of cloud computing services. ISO 27018 is the first and only of its kind in the world, a set of rules built on the ISO 27001 and 27002 standards to ensure the compliance of public cloud providers with the principles and rules established in Directive 95/46/EC. The stated goal of this standard is to serve as a practical *privacy by design* answer to key issues of both legal and contractual nature related to the management of personal data in distributed IT infrastructures following the public cloud model.

Before delving into an analysis of its main characteristics, a brief discussion concerning ISO 27018's predecessors, the ISO 27001 and 27002 standards, is necessary considering that the standard in question represents a *lex specialis* in that it is derived from the principles and procedures put forth by the standards cited above.

I. The foundations of ISO 27018: the ISO 27001 and 27002 standards

The **27001** standard is designed for organizations that intend to adopt a risk management policy for their IT systems (Information Security Management System, ISMS). It establishes a set of generic requirements that the holders of the certification are required to observe in order for the information contained in their IT systems to be considered secure. It does not, however, distinguish between certified entities by nature, nor by size.

At a higher level of precision, the **ISO 27002** standard is integrated through which, starting from an analysis of the specific risks of their IT systems, certified institutions:

- Establish specific security controls, which can be drawn from those contained in the standard or developed based on personalized needs in compliance with the standard;
- Develop their own guidelines for the management of information security.

ISO 27002 is the standard by which the ISO 27018 departs and to which it refers, even if not specifically stated.

II. Why ISO 27018

The use of cloud computing services has become an essential driver of efficiency for a significant number of both commercial and public entities. Beginning several years ago in view of the diffusion of this computational model, the European data protection authorities warned data controllers - typically clients of the largest and most organized cloud providers in terms of economic, technical and legal aspects – against the risks posed by limited transparency of both the modalities of processing as well as transparency regarding the subjects who process the data, not to mention the loss of control over personal information stored in the "cloud".

During the Article 29 Working Party meeting, in fact, the European Data Protection Authorities concluded that "By committing personal data to the systems managed by a cloud provider, cloud clients may no longer be in exclusive control of this data and cannot deploy the technical and organizational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data" (Opinion 5/2012 on Cloud Computing, p. 5).

ISO 27018 is part of this risk scenario and introduces a number of measures, procedures and controls through which the cloud service providers guarantee compliance with the European Directive governing the processing of personal data, reassuring potential buyers of the ability to always control the processes personal data undergo within the cloud provider's systems in complete transparency.

The standard also allows potential buyers to verify the position of the seller with respect to privacy obligations, through examination of documents provided by an independent third

party following 27001 audits, or by reviewing the periodic letter with which ISO guarantees that the certified entities have implemented all the controls provided for in the 27018 standard.

This procedure has been explicitly recommended by the European Data Protection Authorities in the opinion cited above: "Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion" (Opinion 5/2012, p.22). It should therefore be considered as a best practice that will greatly aid both the credibility and reputation of the cloud providers that adhere to it, given that it appears to provide complete evidence of the certified provider's conformity with the privacy principles set out in the Directive.

A provider of a cloud service audited to be compliant with ISO 27018 must specifically guarantee that:

- **The data subject can exercise their rights with regards to the Controller, despite that their data are processed by an external data processor and in a cloud**. In accordance with the standard, the Data Controller is specifically obliged to provide its client with the appropriate tools to ensure the exercise of the rights of the parties to whom the data relate.
- **The methods of processing are exactly the same as those set out in the policy made known to the purchaser of services from the start**, with the express provision that if a change of means becomes necessary for technical reasons, the customer will be promptly informed and have the power to oppose them or to terminate the contract.
- **The personal data in the cloud are not processed for direct marketing or advertising purposes,** unless explicit consent from the data subject has been obtained. **In any case, it can never be a precondition imposed by the supplier on the customer for the provision of the service.**
- **Customers immediately know the names of any sub-processors,** and the place in which they are established, and hold the right to object to any changes in the chain of subcontractors or their country of establishment. The option to terminate the contract in light of these changes may also be provided for.

- **Customers receive timely notices concerning any violations of personal data** (data breaches), in order to give notice to the supervisory authorities (and data subjects) within the timeframe prescribed by law.
- **The methods used to return data to the client once the contract is terminated are regulated** (i.e. Transfer back).
- **Its services are subject to periodic compliance audits** of the employed security standards, evidence of which is provided to customers.
- **All personnel that process personal data are bound by confidentiality agreements** (non-disclosure agreements) and receive appropriate training.

The rules outlined above align the processing of personal data in the "cloud" to the highest standards and regulatory principles in the field. They provide a contractual remedy for the most common cloud service-related problems, often characterized by offers and conditions specified by the suppliers which are not negotiable by customers, frequently incompatible with the obligations that the customer of the cloud service undertakes as Data Controller by operation of applicable privacy law. In adhering to ISO 27018, the cloud provider reports its availability to incorporate the values of European legislation on the protection of personal data to (potential) customers, and testifies to the absolute utility of this standard with respect to the strategy outlined by the European Commission in its communication entitled "Unleashing the potential of cloud computing in Europe", in which the European Commission had the objective of developing a European standard for cloud supplier certification in Europe. ISO 27018 is obviously not the final product of that strategy, but will provide a standard of comparison of utmost quality, a result of the strength and the value of its norms.

It should nonetheless be noted that adherence to ISO 27018 by a provider does not necessarily translate into the transposition of its provisions in the contract which remains entrusted to the parties. However, while such a transposition cannot be automatically inferred, ISO 27018 provides customers with a high quality cloud "checklist" for purchasing cloud services, a document that can be referred to for a detailed comparison with the primary privacy legislation applicable to the provider as well as to assess its "employability".

III. No marketing in the cloud and data breach notification

Among the provisions of the standards listed above, two are of particular importance.

The first is that which prohibits the cloud service provider from processing the data entrusted to them for marketing purposes not previously accepted by the concerned parties – such conduct would be illegal in the European legal context – **and also requires that the supplier does not condition the provision of cloud services on the possibility of direct marketing to the data subjects,** whose data are processed by the client-controller for its legitimate purposes. **This rule incorporates the principles of purpose and proportionality of processing enshrined in European law at its highest level, the Charter of Fundamental Rights,** because on the one hand, it requires that personal data shall not be processed for purposes other than those for which they were collected, and on the other hand stands as an obstacle to unnecessary processing of personal data by the cloud service provider.

The second notable norm is that which requires providers to **notify their clients of a data breach,** in so far as it anticipates the content of Articles 31 and 32 of the draft European Regulation on the protection of personal data which is currently under discussion in Brussels. Once in force, these rules will generalize the obligation for all data controllers to notify the supervisory authorities and the persons concerned in the event of breaches of personal data processed by them, while the European standard applicable today (Directive 2002/58/EC on privacy in electronic communications) requires such reporting only by providers of electronic communications services accessible to the public. The latter also undoubtedly constitutes a best practice to secure benefits for suppliers and customers of cloud services.

IV. Further observations and conclusions

In order to complete the analysis carried out thus far, it should be noted that ISO 27018 does not replace any of the legal bases required today for the transfer of personal data abroad (e.g. Standard contractual clauses, Binding Corporate Rules, Safe Harbor etc.). It will be the

responsibility of the Data Controller to ensure that the transfer of data outside the European Union complies with one of the conditions imposed by Directive 95/46/EC.

Ultimately, it can be concluded that ISO 27018 constitutes an innovation that helps make the varied landscape of contracts and cloud service providers intelligible with the objective of protecting and enhancing personal data.