Privacy Cloud Certification Forecasts Bright Future for Cloud Computing

Bojana Bellamy, CIPP/E
Privacy Perspectives | **Mar 12, 2015**

In February, Microsoft announced that all its cloud enterprise offerings—Office 365, Azure, CRM Online and Intune—were certified by independent third-party auditors for compliance with the new ISO privacy cloud standard 27018. This makes Microsoft the first cloud provider to have received this external certification. Likely, other large and smaller cloud providers will follow suit.

The new ISO cloud standard was adopted in the summer of 2014. The standard includes a set of privacy and security controls for data processing by cloud providers. It also allows for certification and auditing by an independent third party.

Microsoft's certification under this standard is not only an important milestone for Microsoft and its users, but also for cloud providers and users generally, as well as for privacy regulators. In fact, it's a major step forward for privacy. Why is this?

First, ever since its adoption, it was expected that the new ISO privacy cloud would have the potential to shake things up in the world of cloud computing and privacy compliance. As explained in my December post for *Privacy Perspectives*, the standard signified a new stage for corporate privacy accountability, with practical, legal and commercial benefits for both cloud providers and cloud users. Now that Microsoft has actually implemented the standard in respect of its cloud enterprise offerings and received third-party ISO 27018 certification, the expectations are proving to be correct, and it is now confirmed that independently verifiable accountability in the cloud can actually work.

Second, the certification demonstrates that the ISO cloud standard is not a castle in the air; it is practical and imposes concrete substantive requirements on cloud providers

around issues such as customer control, transparency concerning data use and government access to data, data security and limitations on use of data for advertising purposes. It also compels certified cloud providers to put in place an internal compliance infrastructure that implements these requirements and to maintain on going compliance with annual recertification.

Third, the certification under the standard will provide practical benefits for cloud users, providers and others in the cloud chain, such as cloud integrators and resellers.

- It will alleviate key privacy and security concerns associated with cloud technology, including concerns over lack of transparency, control and trust on the part of cloud customers.

- The ability of cloud providers to demonstrate compliance with the standard through third-party certification will facilitate procurement and due diligence processes for those seeking cloud services. It will undoubtedly aid commercial contract negotiations for cloud services and will obviate the need to conduct customer-specific audits.

- Certification to the standard will also go a long way toward delivering legal compliance for both cloud customers and cloud providers. Cloud customers, as controllers, will be in a better position to demonstrate compliance with any legal requirement to select service providers/processors that provide adequate privacy and security safeguards. Cloud service providers, in turn, will improve their ability to show compliance with applicable privacy and security requirements as well as with contractual obligations; cloud providers, as processors, are bound by contractual and sometimes direct legal requirements, many of which are now contained in the new standard.

Fourth, Microsoft's pioneering certification, coupled with the anticipated flood of similar certifications by other providers, will prove that innovative, co-regulatory

accountability mechanisms are valuable complements to existing legal norms. Standards created through multi-stakeholder processes that are consistent with widely accepted legal norms will likely be applicable in any country. Thus, such global standards will, in effect, create bridges between different privacy and security regimes and will enable cloud providers and their customers to reap the benefits of what is, essentially, a borderless technology.

What's next for the cloud privacy standard?

Data privacy regulators and policy-makers have long been asking for standardization and adoption of cloud privacy standards to address challenges of cloud technology. Now that the ISO has succeeded in creating a global consensus standard, and now that cloud providers are starting to implement and certify compliance with the standard, data privacy regulators should be vocal in endorsing and promoting the standard.

Use of certified cloud providers and the implementation and certification of the standard by cloud providers can play a significant role in demonstrating compliance with local privacy laws, including European data protection laws and many other privacy laws that follow the European model. Also, regulators should take ISO cloud certification into account in the context of privacy investigations or enforcement actions as a mitigating factor.

In addition, ISO cloud certification could provide an additional legal basis for cross-border data transfers in countries that regulate data exports. In fact, the newly proposed EU regulation already envisions that seals and certifications can legitimize data transfers. This is a progressive and promising development that should be extended to standards that are substantively similar to the European data protection requirements, as is the case with the ISO cloud privacy standard.

From a cloud provider's perspective, there should be no doubt that they will experience tangible benefits for going above and beyond by certifying under the new standard. In fact, I predict that this particular ISO certification will become a default requirement

and essential component of due diligence for any procurement department seeking cloud services, just like the familiar ISO series 2700 security standards.

Finally, from a wider policy perspective and to work toward global harmonization and interoperability, countries that are developing new privacy laws should recognize and implement a broad range of accountability mechanisms, including standards such as the new ISO cloud standard, as well as privacy seals and marks, certifications, binding corporate rules, cross-border privacy rules and internal or external codes of conduct.