Published on *The National Law Review* https://natlawreview.com

ISO’s New Cloud Privacy Standard - International Standards Organization

Article By:

Inside Privacy Blog at Covington and Burling

This summer, the **International Standards Organization (ISO)** adopted a new voluntary standard governing the processing of personal data in the cloud — ISO 27018. Although this recent development has gone mostly unnoticed by the technology and media press to date, the new cloud standard provides a useful privacy compliance framework for cloud services providers that addresses key processor (and some controller) obligations under EU data protection laws.

ISO 27018 builds on existing information security standards, such as ISO 27001 and ISO 27002, which set out general information security principles (e.g., securing offices and facilities, media handling, human resources security, etc.). By contrast, ISO 27018 is tailored to cloud services specifically and is the first privacy-specific international standard for the cloud. ISO 27018 seeks to address such issues as keeping customer information confidential and secure and preventing personal information from being processed for secondary purposes (e.g., advertising or data analytics) without the customer’s approval. ISO 27018 also responds directly to EU regulators’ calls for the introduction of an auditable compliance framework for cloud processors to increase trust in the online environment (see the European Commission’s 2012 Cloud Strategy here).

More specifically, the standard requires cloud providers to, among other things:

- Always process personal information in accordance with the customer’s instructions.
- Only process personal information for marketing or advertising purposes with the customer’s express consent. Such consent cannot be made a condition for receiving the service.
- Help cloud customers comply when individuals assert their access rights.
- Disclose information to law enforcement authorities only when legally bound to do so.
- Disclose the names of any sub-processors and the possible locations where personal

information may be processed prior to entering into a cloud services contract.

- Help cloud customers comply with their notification obligations in the event of a data breach.
- Implement a policy for the return, transfer or disposal of personal data, for instance when the service comes to an end.
- Subject their services to independent information security reviews at scheduled intervals (or when significant processing changes occur).
- Enter into confidentiality agreements with staff who have access to personal data and provide appropriate staff training.

In order to be certified under ISO 27018, a cloud service must undergo an audit by an accredited certification body. Would-be cloud customers can verify a provider's compliance with the standard via the provider's certificate of conformity. To maintain its certification, a cloud services provider must subject itself to periodic third-party reviews.

Significant cloud players in the United States and Europe have already announced their plans to certify their key cloud services. It remains to be seen if others will follow in their steps and whether ISO 27018 will become a true privacy differentiator in the cloud space.

National Law Review, Volume IV, Number 267