Microsoft adopts first international cloud privacy standard

Microsoft is the first major cloud provider to adopt the world’s first international standard for cloud privacy. It’s another reason customers can move to the Microsoft Cloud with confidence. The standard in question has important practical benefits for enterprise customers around the world. It’s known as ISO/IEC 27018, and it was developed by the International Organization for Standardization (ISO) to establish a uniform, international approach to protecting privacy for personal data stored in the cloud.

ISO 27018 is built on ISO 27001, an international information security standard that is widely adopted. By following ISO 27001 and the code of practice embodied in 27018, a Cloud Service Provider (CSP) can demonstrate that its privacy policies and procedures are robust and in line with the highest standards. Microsoft has a longstanding commitment to follow ISO/IEC27001.

Microsoft continuously expands and improves our enterprise cloud services’ compliance with numerous industry standards and best practices. As part of these efforts, Microsoft Azure, Microsoft Office 365, and Microsoft Dynamics CRM Online services have again successfully passed their annual audit against ISO 27001 by the British Standards Institution (BSI), an independent auditor. As part of this year’s audit, BSI independently validated that each service has now incorporated all of the controls that embody ISO 27018. And similarly, Bureau Veritas has done the same for Microsoft Intune. Microsoft is the first major cloud provider to have incorporated the ISO 27018 standard and code of practice.

The ISO 27018 controls include, for example, guidance that personal information not be used by the service provider for the purposes of marketing and advertising without express consent, and that any subcontractors used by the service provider to process personal information be disclosed to the customers in advance.

ISO 27018 is “advertising-free”
CSPs complying with ISO 27018 cannot use customer data for such purposes as advertising and marketing without the customer’s express consent. Moreover, the provider must not require customer consent to advertising as a condition of the customer’s use of the service. Microsoft has a longstanding commitment not to use data processed by its commercial cloud services for advertising purposes.

ISO 27018 guides the CSP to define its policy for the return, transfer, and/or secure disposal of personal information
As a best practice under ISO 27018, the CSP should establish a retention period after which customer data will be permanently returned or deleted and removed from all services. After a customer subscription ends, Microsoft retains customer data for 90 days and deletes them within 180 days.

ISO 27018 and disclosure of sub-processors
ISO 27018 guides CSPs to disclose the identities of any sub-processor they engage who process personal data. And, if anything changes, the CSP should inform customers promptly to give them an opportunity to object and terminate their agreement.

Microsoft is fully committed to ISO 27018 compliance
In order to be certain of ISO 27018 compliance, CSPs must go through an assessment process and, to remain compliant, must undergo yearly third-party reviews. Microsoft is fully committed to participation in audits and ongoing reviews.

1 Customers can request a copy of the Microsoft Statement of Applicability and audit report applicable to each service to verify the new controls are included in the scope of the respective service’s ISO/IEC 27001:2013 certificate. The certificates for Azure, Office 365 and Dynamics CRM Online are available on the BSI website (http://www.bsigroup.com/).