The new standard, ISO/IEC 27018 (ISO 27018), strengthens data privacy by adding key protections for sensitive customer information stored in the cloud. Published July 30th, 2014 by the International Organization for Standardization (ISO), it sets forth guidelines for cloud service providers concerning Personally Identifiable Information (“PII”). The standard was developed in consultation with contributors from 14 countries and 5 international organizations.

Modernizing security and privacy in the cloud

Before ISO/IEC 27018, there wasn’t a robust, internationally-recognized benchmark for protecting cloud stored PII. The well-established ISO/IEC 27001:2013 international standard provides a flexible system for identifying information security risks and choosing controls to address them. As an addendum to ISO/IEC 27001, ISO/IEC 27018 provides specific guidance to Cloud Service Providers (CSP) for assessment of risks and implementation of state-of-the-art controls for protection of PII stored in the cloud.

Why does an international standard matter?

It is critical that new guidance and controls for PII be defined in international standards. International standards provide at least three key characteristics.

- **Trust.** International standards are created according to strict rules that ensure multiple stakeholders participate in an extensive review process.

- **Acceptance.** International standards from ISO are accepted by all but a few governments as a basis for policy, procurement and trade rules.

- **Global reach.** The global acceptance of ISO standards supports cross-nation business and trade.

Why does adopting ISO 27018 controls matter?

- A cloud service’s audited compliance with the controls in ISO/IEC 27018 gives customers an easy way to confirm that the personal information they entrust to the CSP will be used only as they approve and is kept secure. This is particularly important for government customers, who are often subject to stricter obligations to protect information in their care.

- The ISO/IEC 27018 standard supports regulations set by data protection authorities around the world. Since the standard incorporates the input of multiple regional regulators, use of cloud services that comply with it demonstrates support for the requirements of many local Data Protection Authorities. This standard brings a welcome degree of uniformity to the industry, and adds...
needed protections to improve PII security and compliance in an increasingly cloud-based information environment.

• ISO/IEC 27018 gives new, clear guidance based on EU Data Protection Authorities input on how a data processor should protect customer data, including a requirement that providers must either not mine customer data for advertising purposes, or gain explicit consent to do so. Moreover, it must be possible for a customer to use the service without submitting to such use of personal data for advertising or marketing.

• ISO/IEC 27018 helps customers and CSPs by ensuring that concrete guidance and specific controls for processing PII are addressed as part of an ISO/IEC 27001 audit. Adding the guidance and controls of ISO/IEC 27018 to third-party audits provides evidence of that commitment.

Cloud service providers adopting ISO/IEC 27018 must operate under six key principles:

1. Consent: CSPs must not process the personal data they receive for purposes independent of the instructions of the customer, and they must not use that personal data for advertising and marketing unless expressly instructed to do so by the customer. Moreover, it must be possible for a customer to use the service without submitting to such use of its personal data for advertising or marketing.

2. Control: Customers have explicit control of how their information is used.

3. Transparency: CSPs must inform customers where their data resides and make clear commitments about how that data is handled.

4. Accountability: The standard asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of PII.

5. Communication: In case of a breach, CSPs should notify customers and keep clear records about the incident and the response to it.

6. Independent and yearly audit: A successful third-party audit of a CPS’s compliance documents the service’s conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, the CSP must subject itself to yearly third-party reviews.

A cloud service provider’s adherence to ISO/IEC 27018 controls means the following:

• Customers will always know where their data may be stored and who is processing that data. Customers are sometimes subject to information security rules that restrict where data can be stored. Because ISO/IEC 27018 requires certified CSPs to inform customers of the countries where their data may be stored, customers will have the visibility they need to ensure compliance with applicable rules. The standard also requires CSPs to be upfront about the identities of any subcontractors they engage to help with processing PII before customers enter into a contract. And if any of this changes, the CSP
is required to inform customers promptly to give them an opportunity to object or terminate their agreement.

- **Customers won’t need to worry that the CSP will use their information for marketing and advertising without their consent.** Some CSPs use cloud customer data for their own independent commercial purposes, including for targeted advertising. To make sure that the customer is always in control, ISO/IEC 27018-compliant CSPs may not use customer data for advertising or marketing purposes absent explicit consent from the customer, which cannot be a condition for receiving the cloud service. The choice should always be with the customers.

- **Customers can be confident that the CSP will be transparent about its ability to return, transfer, or securely dispose of any personal data at their request.** Customers are often concerned that cloud services will lead to “lock in,” reducing flexibility and nimbleness over time and creating a system captive to a single standard, software tool, or system. ISO/IEC 27018 requires the CSP to implement a policy to allow for the return, transfer and/or secure disposal of personal information, within a reasonable period of time.

- **Customers can rely on an ISO/IEC 27018 compliant CSPs to help them to handle access, correction or deletion requests.** EU data protection law imposes certain requirements on CSPs – including to allow individuals whose personal information they hold to access that information, to correct it, and even to delete it. Fulfilling these obligations can be a challenging task where an organization has its data stored in a third-party’s cloud. The compliant providers are required to help customers meet these obligations.

- **Customers can rely on ISO/IEC 27018 compliant CSPs to notify them in the event of a security incident resulting in unauthorized PII disclosure, and to help them comply with their notification obligations.** The compliant providers must specify how quickly they will notify their customers of an unauthorized disclosure of PII and how they will help their customers fulfil their notification obligations. ISO/IEC 27018 also requires CSPs to record the type, timing and consequences of any security incidents, to whom the incident was reported, the steps taken to resolve the incident, etc. – creating a record that will in turn assist customers in meeting their reporting obligations.

- **Customers can be confident that an ISO/IEC 27018 compliant CSP will only comply with legally binding requests for disclosure of their data.** The CSP will reject any requests for the disclosure of customers’ personal data that are not legally binding. And if it needs to comply with a legally binding disclosure request (e.g., in relation to criminal investigations), it must always notify the relevant customer, unless prohibited from doing so by law.

- **Customers can rely on independent third party verification of the principles above.** In order to be verified as ISO/IEC 27018-compliant, CSPs must go through a rigorous ISO/IEC 27001 certification process by an accredited independent certification body. **To remain compliant, the CSP must subject itself to yearly third-party reviews.** An ISO/IEC 27018-compliant provider is required to provide customers – prior to commencement of and for the duration of the contract – with independent evidence that controls are implemented in accordance with its policies.
Has Microsoft adopted the new standard for all its services?

Microsoft Azure, Microsoft Office 365, Microsoft Intune and Dynamics CRM Online have already been audited recently to confirm each service has incorporated all of the ISO 27018 controls. Microsoft is the first major cloud provider to successfully undergo an audit including 27018 controls. The additional ISO 27018 controls will be part of our contractual commitment to maintain a data security policy that complies with ISO 27001.