ISO/IEC 27018 (ISO 27018): A Modern Approach to Cloud Security & Privacy

The new standard, ISO 27018, will strengthen data privacy by adding key protections for sensitive customer information stored in the cloud. Published in July 2014 by the International Organization for Standardization, ISO 27018 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 & Privacy in the Cloud
Before ISO 27018, there wasn't a robust, internationally-recognized benchmark for protecting cloud stored PII. The well-established ISO/IEC 27001:2005 standard provides a flexible system for identifying overall information security risks and choosing controls to address them. As an addendum to ISO 27001, ISO 27018 provides specificity to cloud service providers for assessment of risks and implementation of state-of-the-art controls for protection of PII stored in the cloud.

Key Elements of ISO 27018 and the Benefit to Customers
Cloud service providers adopting the new standard must operate under a stronger, industry-wide framework of key principles:

- **Consent**: As part of ISO 27018, cloud providers must not use the data they receive for purposes of their own 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.
- **Transparency**: Cloud providers must inform customers where their data resides and make clear commitments about how that data is handled.
- **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.
- **Communication**: In case of a breach, cloud providers should notify customers and regulators, and keep clear records about the incident and the response to it.
- **Independent Audit**: A successful third-party audit of a cloud service's compliance with 27018 documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations.
- **Control**: Customers have explicit control of how their information is used.

Streamlined Standard
The ISO 27018 standard creates a more streamlined system for adhering to regulations set by data protection authorities around the world. Since the standard incorporates the input of multiple regional regulators, embracing the standard will help demonstrate adherence to the requirements of *any* individual Data Protection Authority's requirements. The ISO 27018 standard brings a degree of uniformity to the industry, and adds needed protections to improve PII security and compliance in an increasingly cloud-based information environment.

July 30, 2014