INFORMATION INTEGRITY SOLUTIONS

www.iispartners.com

ISO/IEC 27018 Primer

What is ISO/IEC 27018?

ISO/IEC 27018 is the first international standard comprising a set of privacy and security controls and guidelines for cloud vendors that process and store personal information on behalf of cloud customers in the public cloud.

Why is ISO/IEC 27018 useful?

ISO/IEC 27018 serves as a helpful reference point for cloud customers seeking a trustworthy cloud solution. For cloud vendors, the standard presents a way to differentiate themselves by adopting a set of credible, controls for the protection of their customers' personal information, which can be verified through independent audits.

How does ISO/IEC 27018 work?

ISO/IEC 27018 references existing controls in the ISO/IEC 27002 code of practice for information security management and introduces new controls and guidelines specifically for protecting personal information in the public cloud. The controls are suggestive, rather than prescriptive.

What are the key elements?

- Support cloud customers' privacy obligations, such as enabling access, correction and erasure by individuals
- Process personal information only in accordance with the cloud customer's instructions
- Notify the cloud customer of law enforcement disclosure requests, where legally permissible
- Reject non-legally binding requests to disclose personal information and consult with the cloud customer first where possible before disclosing personal information
- Seek consent from the cloud customer and ensure proper controls are in place when engaging sub-contractors
- Refrain from using personal information for marketing without express consent of the cloud customer
- Promptly notify the cloud customer of unauthorised access to personal information, or an event that results in its loss, disclosure or alteration
- Develop a policy for the return, transfer, retention and disposal of personal information
- Encrypt data when using portable devices and transmitting over public networks
- Specify and document the countries in which personal information may be stored, including by sub-contractors
- Refrain from unilaterally varying the contract to reduce technical and organisational measures for privacy and security protection