ISO/IEC 27018 PRIVACY SNAPSHOT – HONG KONG

In August 2014 the International Organization for Standardization published a new standard, ISO/IEC 27018, specifically setting out how cloud service providers ("**CSPs**") should protect and manage personal data on behalf of their cloud customers.

If a cloud customer engages a CSP that complies with ISO/IEC 27018, the cloud customer can be confident that moving to the CSP's cloud solution will enable the customer to continue to comply with its key privacy obligations under local privacy laws.

HONG KONG SNAPSHOT: Microsoft complies with the controls in ISO/IEC 27018, so the good news is that Microsoft's cloud customers in Hong Kong can be confident that their use of Microsoft's cloud services enables them to continue to comply with the relevant obligations in Hong Kong's privacy law.

FACTS:

What is the privacy law in Hong Kong? The Personal Data (Privacy) Ordinance ("**PDPO**").

Who is the relevant regulator? The Office of the Privacy Commissioner for Personal Data.

HOW ISO/IEC 27018 HELPS COMPLIANCE:

Microsoft complies with the controls in ISO/IEC 27018. So how exactly does this help Microsoft's cloud customers in Hong Kong to comply with their key privacy law obligations? The comparison table below shows that the customer's key obligations under the PDPO and its Data Protection Principles ("**DPPs**") are matched by the controls ISO/IEC 27018 places on CSPs.[1]

Customer's PDPO obligations	Does ISO/IEC 27018 help compliance? How?
1. Consent and Purpose Generally, a cloud customer must obtain the consent of a data subject in order to collect and process personal data and must only use the personal data for the purposes for which it was collected (DPPs 1 and 3).	**Yes** ISO/IEC 27018 requires the CSP to process personal data in accordance with the cloud customer's instructions and prohibits processing for any other purposes (A.2). The obligation to obtain consent remains the cloud customer's responsibility.
2. Data retention A cloud customer must retain personal data only for as long as is necessary to fulfill the purpose for which it was	**Yes** ISO/IEC 27018 requires the CSP to implement a policy to erase personal data when it is no longer required by the cloud customer (A.5).

[1] This document is not legal or regulatory advice and does not cover any other guidelines or sector specific rules.

Customer's PDPO obligations	Does ISO/IEC 27018 help compliance? How?
collected (DPP 2).	
3. Security The cloud customer must make reasonable security arrangements to prevent unauthorized or accidental access or loss, of personal data (DPP 4).	**Yes** ISO/IEC 27018 requires the CSP to implement security measures to prevent unauthorized access, collection, use or disclosure, of personal data (5 to 13 and A.10).
4. Sub-contracting The cloud customer may use sub-contractors to process personal data on its behalf as long as the cloud customer ensures that the personal data is protected to the same level as required by the PDPO (DPP 4).	**Yes** ISO/IEC 27018 requires the CSP to execute a contract with any sub-contractors that includes the same security and personal data protection obligations of the CSP (A.10.12).
5. Data subjects' right of access and correction The cloud customer must, upon request, provide access to and/or correct the data subject's personal data (DPP 6, and Sections 18 and 22).	**Yes** ISO/IEC 27018 requires the CSP to assist its cloud customer to comply with a data subject's access and/or correction requests (A.1).
6. International transfer A cloud customer may transfer personal data outside of Hong Kong. Section 33 is not yet in force. However, it is best practice to comply with its provisions, which means that personal data may be transferred outside of Hong Kong if the cloud customer has taken all reasonable precautions to ensure that the personal data is treated to a standard of protection that is comparable to the PDPO.	**Yes** ISO/IEC 27018 requires the CSP to apply the same exacting standards to the personal data, no matter where the personal data is processed (Generally and A.11).