Microsoft's Data Protection Compliance

Microsoft

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

FACTS:

What is the privacy law in Malaysia?
The Personal Data Protection Act 2010 ("PDPA"). The PDPA took effect in February 2014.

Who is the relevant regulator?
The Personal Data Protection Commissioner

Are there international standards on data privacy and cloud computing?
Yes. 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.

Has Microsoft been certified as complying with ISO/IEC 27018?
Yes. Microsoft was the first major cloud provider to adopt the standard.

Does Microsoft offer contractual commitments on data privacy to its cloud customers?
Yes. Many of Microsoft's contractual commitments for commercial customers are set out in the Online Service Terms ("OST") document, which is available for download from the Microsoft Volume Licensing website (www.microsoftvolumelicensing.com).

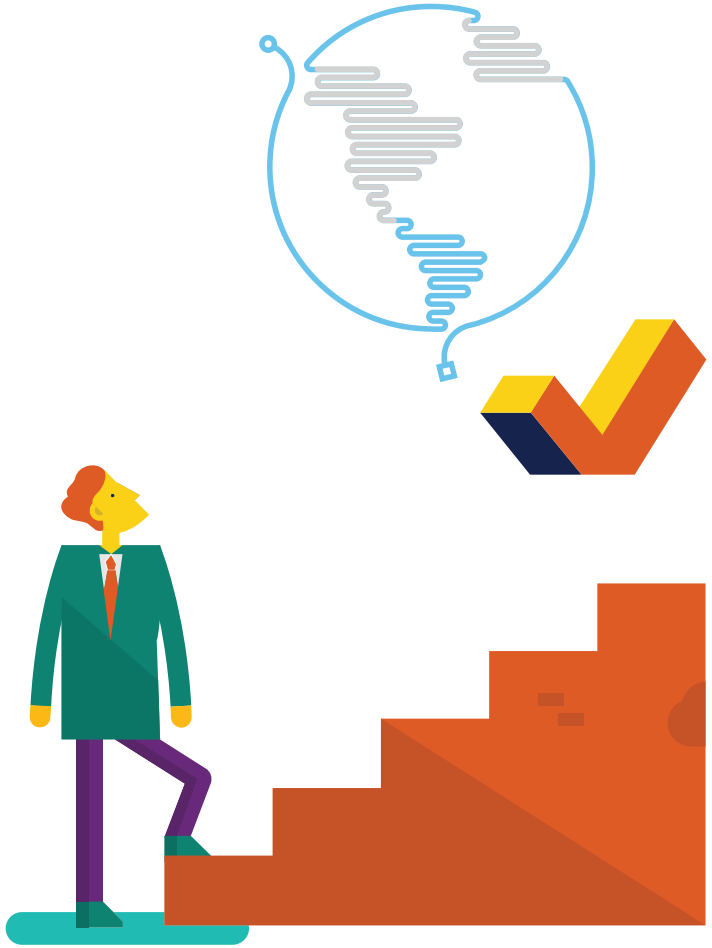
Where can I learn more about Microsoft's commitment to data privacy?
In addition to this document, please consult the following websites or speak to your Microsoft account executive:

Office365 Trust Center: http://trustoffice365.com

Azure Trust Center: http://www.windowsazure.com/en-us/support/trust-center/

Dynamics CRM Online Trust Center: http://www.microsoft.com/en-us/dynamics/crm-trust-center.aspx

Microsoft Privacy portal: http://www.microsoft.com/privacystatement/en-us/core/default.aspx



How ISO/IEC 27018 Helps Compliance:

Microsoft

Microsoft complies with the controls in ISO/IEC 27018. So how exactly does this help Microsoft's cloud customers in Malaysia to comply with their key privacy law obligations? Where do Microsoft's contracts reflect these commitments? The comparison table below shows that the customer's key obligations under the PDPA as they relate to outsourcing of data processing are matched by the controls ISO/IEC 27018 places on CSPs[1] and includes reference to relevant provisions from Microsoft's volume licensing contracts.

Customer's PDPA obligations	Does ISO/IEC 27018 help compliance? How?	What do Microsoft's contracts say?
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 (Section 6).	**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.	"Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data." (OST, p. 7[2])
2. Disclosure A cloud customer must not, without consent of the data subject, disclose personal data for any purpose not directly related to the purpose for which it was to be disclosed at the time of collection (Section 8).	**Yes** ISO/IEC 27018 requires the CSP to process the personal data only in accordance with the cloud customer's instructions (see above) and to reject requests for disclosures that are not legally binding (A.5).	"Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data." (OST, p. 7) "Microsoft will not disclose Customer Data to law enforcement unless required by law." (OST, p. 7) "Upon receipt of any other third party request for Customer Data (such as requests from Customer's end users), Microsoft will promptly notify Customer unless prohibited by law. If Microsoft is not required by law to disclose the Customer Data, Microsoft will reject the request." (OST, p. 7)

[1] The contents of this document are for informational purposes only. They do not contain legal or regulatory advice and should not be relied on as such. Microsoft encourages its customers to seek independent legal advice to ensure that their internal processes comply with the requirements of the PDPA and any other guidelines or sector-specific rules.

[2] References are to the July 2015 version of the OST.

Customer's PDPA obligations	Does ISO/IEC 27018 help compliance? How?	What do Microsoft's contracts say?
3. Security The cloud customer must take practical security steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, including obtaining sufficient guarantees from any CSP that it has technical and organizational security measures in place to protect the personal data (Section 9).	**Yes** ISO/IEC 27018 requires the CSP to have robust technical and organizational security measures in place and to take reasonable steps to ensure compliance with those measures. The CSP must implement security measures to prevent unauthorized access, collection, use or disclosure, of personal data (5 to 13 and A.10).	"Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction." (OST, p. 8) For detailed information on Microsoft's contractual security commitments for Office 365 Services, Microsoft Azure Core Services, Microsoft Intune Online Services and Microsoft Dynamics Online Services see OST, pp. 10-12.
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 PDPA (Section 9(2)).	**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).	"Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST." (OST, p. 8)
5. Data retention A cloud customer must retain personal data only for as long as is necessary to fulfill the purpose for which it was collected (Section 10).	**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.9.3).	"Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90 day retention period ends, Microsoft will disable Customer's account and delete the Customer Data." (OST, p. 4)

Customer's PDPA obligations	Does ISO/IEC 27018 help compliance? How?	What do Microsoft's contracts say?
6. 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 (Section 12).	**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).	The obligation to provide access to and/or correct the data subject's personal data is the cloud customer's responsibility. However, Microsoft's contracts do speak to our commitment to help the cloud customer comply with this obligation by ensuring on-demand access to the data. "Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer." (OST, p. 7) Each Online Service is also subject to a Service Level Agreement ("SLA"), which includes financially-backed uptime guarantees of at least 99.9% per month. These SLAs can be downloaded from Microsoft's Volume Licensing website: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?mode=1
7. International transfer A cloud customer may transfer personal data outside of Malaysia if the personal data is treated to a standard of protection that is comparable to the PDPA (Section 129).	**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).	The OST and SLAs apply worldwide and are not limited by where your information is located.