Confidential

HONG KONG – PRIVACY

GUIDANCE ON COMPLYING WITH PRIVACY LAW REQUIREMENTS APPLICABLE TO CUSTOMERS USING CLOUD COMPUTING

Last updated: February 2017

1. WHAT DOES THIS MICROSOFT GUIDANCE CONTAIN?

This guidance document provides a guide for Microsoft customers on meeting their obligations under privacy law requirements in Hong Kong when using cloud computing. Sections 2 to 5 of this guidance set out information about the privacy laws and the requirements that apply in Hong Kong.

Section 6 sets out questions in relation to using cloud computing services based on the privacy laws, regulations and guidance that are relevant to the use of cloud computing services. Although there is no requirement to complete a checklist like this one, we have received feedback from our customers that this checklist approach is very helpful. The checklist can be used:

(i) as a checklist for ensuring compliance with the requirements set out in the laws, regulations and guidelines (listed in Section 2); and

(ii) as a tool to aid discussions with the regulator (listed in Section 3), should the regulator wish to discuss your organization's overall approach to compliance with the privacy law requirements.

Note that this document is not intended as legal or regulatory advice and does not constitute any warranty or contractual commitment on the part of Microsoft or its affiliates. Instead, it is intended to streamline the compliance process for you. You should seek independent legal advice on your use of cloud computing and your legal and compliance obligations. If you have any questions, please do not hesitate to get in touch with your Microsoft contact.

2. WHAT LAWS, REGULATIONS AND GUIDANCE ARE RELEVANT?

In Hong Kong, the key legislation and guidance in this area are:

- The Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**"); and
- Hong Kong Privacy Commissioner Information Leaflet on Cloud Computing (revised July 2015) ("**the Cloud Guidance**").

Field Code Changed

Field Code Changed

Note that the PDPO sets out a number of Data Protection Principles ("**DPPs**") which are also referred to in this guidance.

3. **WHO IS THE RELEVANT REGULATORS?**

The Office of the Privacy Commissioner for Personal Data ("**the Privacy Commissioner**").

Field Code Changed

4. **IS REGULATORY NOTIFICATION OR APPROVAL REQUIRED IN HONG KONG?**

No.

You do not need to notify the Privacy Commissioner or obtain prior approval from the Privacy Commissioner before engaging cloud service providers ("**CSPs**") to provide cloud computing services. Note that the Privacy Commissioner has the power to change this in the future under Section 14 PDPO but we are not aware of any current plans to make such a change.

5. **IS/ARE THERE (A) SPECIFIC FORM OR QUESTIONNAIRE(S) TO BE COMPLETED?**

No.

6. CHECKLIST

Key:

In blue text, Microsoft has included template responses that would demonstrate how your proposed use of Microsoft's services would address the point raised in the checklist. The suggested responses may provide sufficient detail but if you require further information, Microsoft will be happy to provide this if you get in touch with your Microsoft contact. Some points are specific to your own internal operations and processes and you will need to complete these answers as well.

In *red italics*, Microsoft has provided guidance to assist you with the points in the checklist.

No.	Question/requirement	Template response and guidance
A. OVERVIEW		
1.	Who is the proposed CSP?	The CSP is Microsoft Operations Pte Ltd, the regional licensing entity for Microsoft Corporation, a global provider of information technology devices and services, which is publicly-listed in the USA (NASDAQ: MSFT). Microsoft's full company profile is available here.
2.	What data will be processed by the CSP?	*When you choose a Microsoft cloud service, you have full control over the type of data that will be processed by Microsoft. Therefore, the types of data impacted are within your control and the template response will need to be tailored according to the type of data that you have selected to be processed by Microsoft.* We ensure that all data (but in particular any customer data) is treated with the highest level of security in accordance with good industry practice to ensure that we and our service provider comply with our legal and regulatory obligations. We only collect and process data that is necessary for our business operations in compliance with all applicable laws and regulation and this applies whether we process the data on our own systems or via a cloud solution such as Microsoft Office 365 or Microsoft Azure or

Field Code Changed

<table>
<tr><th>No.</th><th>Question/requirement</th><th>Template response and guidance</th></tr>
<tr><td></td><td></td><td>Microsoft Dynamics 365. Typically, the types of data that would be processed and stored by the Microsoft cloud service would include:
<table>
<tr><th></th><th>Type of Data</th><th>Processed/Stored/Both</th><th>Sensitive (Y/N)</th></tr>
<tr><td>1.</td><td>Customer data (including customer name, contact details, account information and correspondence).</td><td>Both</td><td>Y</td></tr>
<tr><td>2.</td><td>Employee data (including employee name, contact details, internal and external correspondence by email and other means and personal information relating to their employment with the organization).</td><td>Both</td><td>Y</td></tr>
<tr><td>3.</td><td>Transaction data (data relating to transactions in which the organization is involved).</td><td>Both</td><td>Y</td></tr>
<tr><td>4.</td><td>Other personal and non-personal data relating to the organization’s business operations.</td><td>Both</td><td>Y</td></tr>
</table></td></tr>
<tr><td>3.</td><td>What service deployment model is being used (i.e. infrastructure as a service (IaaS), platform as a service (PaaS) or software as</td><td>The Cloud Guidance (pg.4) suggests that customers using cloud computing services will consider any risks associated with the service deployment model being adopted. You have a number of cloud service deployment models to choose from. Identifying which cloud service deployment model is the most</td></tr>
</table>

No.	Question/requirement	Template response and guidance
	a service (SaaS))?	*appropriate for your organization depends on your organization's needs and the type of data processing you require.* We will be using: • [Software as a service ("**SaaS**") (e.g. Microsoft Office 365 and Microsoft Dynamics 365); • Platform as a service ("**PaaS**") (e.g. Microsoft Azure SQL Database and Azure App Service); and • Infrastructure as a service ("**IaaS**") (e.g. Azure Virtual Machines and Azure Load Balancer).]
B. DATA COLLECTION AND PROCESSING		
4.	Is the personal data collected by the customer for a lawful purpose directly related to a function or activity of the customer, necessary for or directly related and adequate but not excessive, to that purpose?	*DPP 1(1) PDPO requires that personal data be collected for a lawful purpose directly related to the activity of the data user and the collection of the data is necessary for or directly related to that purpose. DPP 1(1) PDPO also requires that the data collected is adequate and proportionate with the purpose for which it is being collected.* Yes. The types of data we collect and the purposes for which we collect it are set out in our organization's Privacy Policy, which is available at [insert link]. We have comfort that this will not be impacted by our use of Microsoft cloud services. This is because Microsoft commits that it will only use our data to provide the Microsoft cloud services. Microsoft commits that it will not use our data or derive information from the data for advertising or similar commercial purposes.
5.	Has the customer collected the personal data using means that are fair and lawful?	*DPP 1(2) PDPO requires that personal data must be collected by means which are lawful and fair. Examples of obtaining personal data which is considered "unlawful" or "unfair" include obtaining*

No.	Question/requirement	Template response and guidance
		personal data through deception, coercion or by covert means. Yes. The means through which we collect personal data are set out in our Privacy Policy, which is available at [insert link].
6.	Has the customer informed the data subject on or before collecting the data of: a) whether it is obligatory or voluntary to supply the data; b) where it is obligatory to supply the data, consequences for failing to do so; c) the purpose for which the data will be used; d) the classes of persons to whom the data may be transferred; e) the data subjects' right to request access and/or correct their personal data; and f) the contact details of the person to whom requests for access or correction should be sent.	*DPP 1(3) PDPO requires all practicable steps be taken to ensure that on or before collecting data from a data subject that he/she is informed: (i) explicitly or implicitly whether it is necessary to supply the data and when it is necessary, the ramifications for not doing so; (ii) explicitly of the purpose for using the data; and (iii) explicitly of the classes of persons to whom the data may be transferred; DPP 1(3) PDPO also requires all practicable steps be taken to ensure that on or before first use of the data for the purpose for which it was collected from a data subject that he/she is informed: (iv) explicitly of his/her rights to request access and/or correct his/her data; and (v) explicitly of the contact details of the person who handles access and/or correction requests made to the data user. You will need to expand on the answer below depending on the processes you use to inform the data subject of these matters.* Yes. We have informed the data subject of the information as required in items a) to f) of the question on or before collection of his/her personal data. This is primarily dealt with through our Privacy Policy, which is made available to all of our data subjects, at [insert link].
7.	Is there a provision in the contract between the CSP and the customer and in the contract between the data subject and the	*DPP 3(1) PDPO states that personal data of a data subject shall not be used for a new purpose without the prescribed consent of the data subject. Section 2(3) PDPO states that prescribed consent means the express consent of the person that is given voluntarily, and that has not been withdrawn. DPP 3(3)*

No.	Question/requirement	Template response and guidance
	customer which restricts the use of personal data (and any other personal data CSPs or customers may collect during the course of the contract) for a new purpose without the prescribed consent (i.e. express and voluntary consent) of the data subject, unless the customer has reasonable grounds for believing that the use of that data for such new purpose is clearly in the interest of the data subject?	*PDPO states that a data user must not use the personal data of a data subject for a new purpose even if express and voluntary consent has been given, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject. The Cloud Guidance (pg.4) also suggests that a contract with a cloud provider contains a provision that limits the use of personal data for a purpose that is identical to or directly related to the purpose stated at the time of data collection.* Yes. The purposes for which we use data are described in our Privacy Policy, which is available at [insert link]. This is backed up by our use of Microsoft cloud services, since our data that is hosted in the Microsoft cloud belongs to us. The Online Services Terms of Microsoft ("**OST"**) states that all data (including personal data) that we give to Microsoft will be used only to provide the Microsoft cloud services including purposes compatible with providing those services. For example, Microsoft may use our data to provide a personalized experience, improve service reliability, combat spam or other malware, complete transactions, detect or prevent fraud or improve features and functionality of the Microsoft cloud services. Microsoft will not use our data for purposes that are unrelated to providing the service such as for any advertising or similar commercial purposes.
8.	Will all practicable steps be taken to ensure a person can: a) ascertain the customer's policies and practices in relation to personal data; b) be informed of the kind of personal data held by the customer;	*DPP 5 PDPO requires that all practicable steps be taken to ensure that a person can ascertain: (i) the personal data policies and practices of a data user; (ii) the types of personal data held by a data user; and (iii) the main purposes for which personal data will be used.* Yes, our policies and practices in relation to personal data are set out in our Privacy Policy at [insert link]. We can also readily access Microsoft's policies and practices in relation to personal data through

No.	Question/requirement	Template response and guidance
	c) be informed of the main purposes for which personal data held by the customer are to be used?	resources available at the Microsoft Trust Center. We are also informed about the main purposes for which personal data is used by Microsoft in the OST that is available here.
C. ACCESS, CORRECTION AND DELETION		
9.	What practicable steps does the customer take to ensure personal data is accurate having regard to the purpose it is to be used for?	*DPP 2 PDPO requires that all practicable steps be taken to ensure that personal data held by a data user is not incorrect, misleading, incomplete or obsolete, taking into account the purpose of the use of the personal data. The sample response below provides a few examples of measures you could use to ensure that the personal data is accurate and up-to-date.* Yes, we have taken the following measures to ensure that personal data collected is accurate: • [e.g. users are encouraged to update their details regularly through the "My Account" page of our website]; • [e.g. our Terms of Service require users to ensure that the personal information they provide to us is accurate and to update us regarding any changes to their personal information]; and • [e.g. our Employment Terms require our employees to ensure that the personal information they provide to us is accurate and to update us regarding any changes to their personal information].
10.	Can the data subject ascertain whether or not the customer holds personal data about the data subject?	*DPP 6(a) PDPO and Section 18(1)(a) PDPO require a data subject to be able to determine and be informed about whether a data user holds personal data about him/her. The sample answer below provides some examples of how to meet this requirement but is not intended to be an exhaustive list and will need to be tailored by you depending on your processes.* Yes. The data subject can ascertain whether or not we hold personal data about the data subject. [First,

Field Code Changed

Field Code Changed

No.	Question/requirement	Template response and guidance
		we inform data subjects in advance via our Privacy Policy. Second, after we have collected data, we provide a summary of the data we hold in the "My Account" page of our website which is available to each user. Finally, data subjects can contact us at any time to request details of the data we hold since the relevant process and contact details are set out in our Privacy Policy.] This is not impacted by our use of Microsoft cloud services as we retain control over our data held in the Microsoft cloud and we are able to access or retrieve our data in the Microsoft cloud at all times.
11.	Can the data subject request access to personal data: a) within a reasonable time; b) at a fee, if any, that is not excessive; c) in a reasonable manner; and d) in a form that is intelligible?	*DPP 6(b) PDPO requires that a data subject shall be able to reasonably request access to personal data within a reasonable time at a fee (if any), and in a form that is comprehensible. Fees charged (if any) should not be excessive (i.e. with a view to generate profit or to deter the data subject from exercising his data access right under the PDPO). Section 18(a) PDPO states that a data subject may make a request to be informed about whether a data user holds personal data about him/her.* Yes. The data subject may access personal data within [insert period]. [The data user is required to pay us [insert amount] for each data access request. The process for doing so is set out in our Privacy Policy at [insert link].] We are satisfied that we can comply with access requests from data subjects because we may access or retrieve our data that is held in Microsoft servers at all times. We are also able to download a copy of our data without requiring assistance from Microsoft (e.g. Microsoft Office 365 supports this through supplying import and export wizards for Exchange Online so that end users can download emails, contacts, calendar appointments to their local computers at any time). If our subscription to a Microsoft cloud service ends, Microsoft retains data in a limited function account for 90 days after the end of the contract period, for us to extract our data. After the 90-day retention period ends, Microsoft will delete our data.

No.	Question/requirement	Template response and guidance
12.	Will the customer comply with the data subject's data access request within 40 days after receiving the request?	*Section 19(1) PDPO requires that data user must respond to a data access request within 40 days after receiving the request. You will need to ensure you have the processes internally to meet this requirement.* Yes, we will comply with the data subject's data access request within 40 days after receiving the request. This is not impacted by our use of Microsoft cloud services as we retain control over our data held in the Microsoft cloud and we are able to access, retrieve and edit our data in the Microsoft cloud at all times.
13.	Can the data subject request the correction of their personal data?	*DPP 6(e) PDPO requires that a data subject shall be entitled to request the correction of his/her personal data. Section 22(1) PDPO states that a data subject is entitled to request a correction of personal data in relation to data provided by him/her pursuant to a data access request.* Yes. The data subject may request correction of their personal data and the process for doing so is set out in our Privacy Policy, which is available at [insert link]. This is not impacted by our use of Microsoft cloud services as we retain control over our data held in the Microsoft cloud and we are able to access, retrieve and edit our data in the Microsoft cloud at all times.
14.	Will the correction of personal data be made not later than 40 days after the request from the data subject is received?	*Section 23(1) PDPO requires that a data user who is satisfied that personal data to which a data correction request is made is inaccurate, correct and supply such corrected data to the data subject within 40 days after receiving the request. You will need to ensure you have the processes internally to meet this requirement.* Yes. The personal data will be corrected no later than 40 days after the request from the data subject is received. We can comply with correction requests from data subjects as we retain control over our data held in the Microsoft cloud and we are able to access, retrieve and edit our data in the Microsoft cloud at

No.	Question/requirement	Template response and guidance
		all times.
15.	What are the practicable steps the customer takes to ensure data which is no longer required for the purpose (or any directly related purpose) for which it was used or if the data subject withdraws his/her consent is erased?	*Section 26 PDPO requires that a data user must take all practicable steps to erase personal data that is no longer required for the purpose (including a directly related purpose) for which the data was used unless such erasure of data is prohibited under any law or it is in the public interest for the data not to be erased. Section 2(3) PDPO requires that data be used only with the consent of the data subject. Hence, data should be erased when a data subject withdraws consent by notice in writing.* Our policy allows data subject's data to be erased if the personal data is no longer required for the purpose for which data was used or if the data subject withdraws his/her consent to the processing of his/her data. Our data retention policy is as follows: • [ ]; • [ ]; and • [ ]. In addition, Microsoft enables us to maintain control over the data that we give to Microsoft, which means we can arrange for it to be retained or erased as we deem appropriate, taking into account our regulatory obligations. In particular, we can request for our data that is held on the Microsoft cloud to be deleted at any time. When we terminate our subscription to Microsoft cloud services, Microsoft retains data in a limited function account for 90 days after expiration or termination of our subscription, for us to extract our data. Thereafter, data is deleted. This ensures that our data is deleted within the specified time period so that data privacy is maintained. At a technical level, Microsoft uses best practice procedures and a wiping solution that is National Institute of Standards and Technology ("**NIST**") 800-88 compliant. For hard drives that cannot be wiped, it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or

No.	Question/requirement	Template response and guidance
		incinerate).
16.	Is there a provision in the CSP contract that sets out the duration in which CSP can keep personal data and how personal data is to be erased or returned to customers on request from the customer, contract completion or contract termination?	*DPP 2(3) PDPO requires that a data user must adopt contractual or other measures to prevent any personal data transferred to a data processor from being kept longer than is necessary or required for processing the data. The Cloud Guidance (pg.4) suggests that there be a provision in the contract with a CSP that sets out how personal data is to be deleted or returned to data users upon the termination or expiration of such contract.* Yes. Microsoft commits that it will not retain our data when it is no longer necessary to retain such data. The OST states that when we terminate our subscription to Microsoft cloud services, Microsoft retains data in a limited function account for 90 days after expiration or termination of our subscription, for us to extract our data. Thereafter, data is deleted. This helps ensure that we have plenty of time to migrate this data to other services as required by our business. It also ensures that our data is deleted within the specified time period so that data privacy is maintained.
D. DATA SECURITY		
17.	Will all practicable steps be taken to ensure personal data is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to:	*DPP 4(1) PDPO requires that all practicable steps shall be taken to ensure that personal data held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use taking into account the type of data and the consequences of harm, the physical location of data, any built-in security measures, any measures to control who has access to personal data and any measures to ensure that data is transmitted securely and safely.* Yes. Microsoft provides industry-leading cloud security measures and Microsoft cloud services (e.g. Microsoft Office 365, Microsoft Dynamics 365 and Microsoft Azure) are built on ISO/IEC 27001 and ISO/IEC 27018 standards, which is a set of rigorous global standards covering physical, logical, process and management controls. By partnering with Microsoft, we have taken practicable steps to ensure that

No.	Question/requirement	Template response and guidance
		personal data is protected against unauthorized or accidental access, processing, erasure, loss or use. We expand on this in our responses to (a) to (e), below.
	a) the kind of data and the harm that could result;	Yes. Microsoft ensures that access to sensitive files, commands and services are restricted and protected from manipulation. We can augment our data protection strategy by using rights management service ("**RMS**") that protects sensitive information through persistent usage policies that remain with the information, no matter where they are stored. For example, Microsoft Office 365 includes RMS functionality so that emails, and documents such as those created by Word, Excel and PowerPoint can be RMS protected to help safeguard sensitive information. We can define who can open, modify, print, forward, or take other actions with the information and we can create custom usage policy templates such as "confidential—read only" that can be applied directly to the information.
	b) the physical location of where the data is stored;	Yes. Microsoft ensures that access to datacenter facilities is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multi-factor access control, integrated alarm systems, and extensive 24x7 video surveillance from the operations center. Please refer to our response to question 31 and 32 for more information on how Microsoft selects the location of its data centers and how it responds to requests for our data from law enforcement or other governmental entities.

No.	Question/requirement	Template response and guidance
	c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;	Yes. Microsoft implements traffic throttling to prevent denial-of-service attacks. It uses the "prevent, detect and mitigate breach" process as a defensive strategy to predict and prevent security breaches before they happen. This involves continuous improvements to built-in security features, including port-scanning and remediation, perimeter vulnerability scanning, OS patching to the latest updated security software, network-level DDOS detection and prevention and multi-factor authentication for service access. Microsoft also implements the Microsoft Security Development Lifecycle ("**SDL**") which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft software and services. Through design requirements, analysis of attack surface and threat modelling, SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle.
	d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and	Yes. Microsoft applies strict controls over which personnel roles and personnel will be granted access to our data. Personnel access to the IT systems that store our data is strictly controlled via role-based access control and lock box processes that involve not only approvals from within Microsoft but also explicit approval from us. Access control is an automated process that follows the separation of duties principle and the principle of granting least privilege. This process ensures that the engineer requesting access to these IT systems has met the eligibility requirements, such as a background screen, fingerprinting, required security training and access approvals. Employees of Microsoft who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. In emergency situations, a "Just-In-Time (JIT) access and elevation system" is used (that is, elevation is

No.	Question/requirement	Template response and guidance
		granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service.
	e) any measures taken for ensuring the secure transmission of the data.	Yes. Microsoft uses multiple encryption methods, protocols and algorithms in the Microsoft cloud services to provide a secure path through the infrastructure over which data can travel and to protect the confidentiality of data that is stored within the infrastructure. These include Transport Layer Security/Secure Sockets Layer (TLS/SSL), which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network, and IP Security (IPsec), an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it is transferred across the network. Other encryption technologies used by Microsoft in the Microsoft cloud services include Advanced Encryption Standard (AES)-256, the NIST specification for a symmetric key data encryption that was adopted by the US government to replace Data Encryption Standard (DES) and RSA 2048 public key encryption technology.
18.	Is there an end-to-end, comprehensive and properly managed encryption system?	*The Cloud Guidance (pg.5) suggests that data users are expected to maintain the same level of protection of personal data irrespective of whether the personal data is managed/held by them or by a cloud provider and where data users may not have direct oversight over all the controls necessary for the protection of personal data, data users should consider implementing an encryption system for the transmission and storage of personal data.* Yes. Microsoft cloud services use encryption protocols that are recognized within the industry as highly secured to safeguard our data. Microsoft uses multiple encryption methods, protocols and algorithms in the Microsoft cloud services to provide a secure path through the infrastructure over which data can travel and to protect the confidentiality of data that is stored within the infrastructure. These include TLS/SSL, which uses symmetric cryptography based on a shared secret to encrypt communications as they travel over the network, and IPsec, an industry-standard set of protocols used to provide authentication, integrity, and confidentiality of data at the IP packet level as it is transferred across the

No.	Question/requirement	Template response and guidance
		network. Apart from data in transit, Microsoft is also committed to protect our data at rest with built-in technology such as Encrypting File System and BitLocker, and will provide us with access to further encryption capabilities to encrypt the content stored in Microsoft's cloud services. Other encryption technologies used in the Microsoft cloud services include AES-256, the NIST specification for a symmetric key data encryption that was adopted by the US government to replace DES and RSA 2048 public key encryption technology.
19.	If software as a service (SaaS) is being used, what are the risks of such an arrangement and how can they be mitigated?	*The Cloud Guidance (pg.4) suggests that data users who use SaaS would have to use the software provided by the cloud provider as part of the data user's business tools and may have to adjust their operation in order to use such software or rely on the cloud provider to operate the software, leading to less direct control by the data user over the personal data being processed. Hence, data users using SaaS need to quantify the associated risks and mitigate such risks.* [(Only applies when you have conducted risk assessment) We have carried out a risk assessment and have determined that the risk of adopting a SaaS model is not higher than the risk of deploying local device software.] A SaaS model is also not inherently riskier than other cloud service deployment models (e.g. IaaS or PaaS). The main potential risk to be addressed across our entire technology infrastructure is data security. We are satisfied that the risk in this respect should be assessed based on the service provider and their ability to provide a robust and secure environment rather than purely assessed based on the choice of cloud service deployment model. In this respect, we have selected Microsoft taking heavily into account the fact that it is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even highly sophisticated organizations across all the cloud service deployment models.
20.	Is there a contractual provision in the CSP contract to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred for	*DPP 4(2) PDPO requires a data user to adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to CSP for processing.* Yes. The OST states that Microsoft is committed to helping protect the security of our data and that

No.	Question/requirement	Template response and guidance
	processing?	Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect our data against accidental, unauthorized or unlawful access, disclosure, alterations, loss, or destruction.
21.	Do the services and contract terms of the CSP contract meet all the security and personal data privacy protection standards the customer requires?	*The Cloud Guidance (pg.3) suggests that a data user must carefully evaluate whether the contract terms with a cloud provider meet all the security and personal data protection standards of the data user.* Yes. Microsoft commits in the OST that it has implemented and will maintain security measures relating to the following to protect data that is within the Microsoft cloud and we are satisfied that these measures meet our security and personal data privacy protection standards: • organization of information security (e.g. Microsoft personnel with access to customer data are subject to confidentiality obligations and Microsoft performs a risk assessment before processing any customer data) • asset management (e.g. maintaining an inventory of media on which customer data are stored and restricting access to sensitive information); • human resources security (e.g. security training for Microsoft personnel); • physical and environment security (e.g. restricting physical access to Microsoft's facilities and data centers); • communications and operations management (e.g. Microsoft implements encryption and data recovery procedures); • access control (e.g. Microsoft only permits technical support personnel to have access to customer data when needed and restricts access to customer data to only those individuals who require such access to perform their job functions); • information security in incident management (e.g. service monitoring and an incident response process that includes notification of security breaches); and

No.	Question/requirement	Template response and guidance
		• business continuity management (e.g. Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process customer data are located). More information on the security commitments given by Microsoft in the OST is available here and more information on the security measures implemented by Microsoft is available at the Microsoft Trust Center.
22.	Are there ways to verify the data protection and security commitments made by the CSP?	*The Cloud Guidance (pg.4) suggests that a data user should find ways to verify the data protection and security commitments made by a cloud provider.* Yes. We verify these commitments through the use of international standards. Microsoft cloud services are built based on ISO/IEC 27001 and ISO/IEC 27018 standards and Microsoft undergoes third-party audits by internationally recognized auditors to ensure that Microsoft adheres to such standards. Such third party audits serve as an independent validation that Microsoft complies with such standards for security and privacy and copies of the reports are available at the Service Trust Portal.
23.	Is there a provision in the CSP contract which requires the CSP to notify the customer of any data breaches?	*The Cloud Guidance (pg.5) suggests a data user to ensure that the contract with a CSP obliges the CSP to notify the data user of any data breach.* Yes. The OST states that if Microsoft becomes aware of any unlawful access to our data stored on Microsoft's equipment or facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of our data, Microsoft will promptly notify us of the security incident.
24.	Does the CSP provide any mechanism for timely handling in case of data breaches, such as to take speedy remedial action, to maintain business continuity, to meet legal	*The Cloud Guidance (pg.5) suggests that any mandatory notification by CSPs would facilitate timely handling of data breaches by data users and ensure business continuity.* Yes. Besides promptly notifying us of any security incident, Microsoft has committed in the OST that it

Field Code Changed

Field Code Changed

No.	Question/requirement	Template response and guidance
	obligations and to manage customer and public relations?	will investigate the incident and provide us with detailed information about the security incident and take reasonable steps to mitigate the effects and minimize any damage resulting from the security incident.
E. SUBCONTRACTING		
25.	What are the sub-contracting arrangements?	*The Cloud Guidance (pg. 3) suggests a data user to ascertain the sub-contracting arrangements of a CSP.* Microsoft hires sub-contractors to provide certain limited or ancillary services on its behalf. Any such sub-contractors will be permitted to obtain our data only to deliver the services Microsoft has retained them to provide and will be prohibited from using our data for any other purpose. Microsoft discloses the names of sub-contractors who have access to our data at the Microsoft Trust Center and provides advance notice of any new sub-contractors.
26.	Is there contractual assurance in the contract with the CSP that the same level of technical and administrative protection and monitoring and remedial actions compliance controls will be equally applicable to sub-contractors?	*The Cloud Guidance (pg.3) suggests that a data user should obtain formal contractual assurance from the CSP that its sub-contractors will implement the same level of protection and compliance controls over personal data as the CSP.* Yes. The OST states that Microsoft remains responsible for its sub-contractors' compliance with Microsoft's obligations in the OST. As part of the OST, Microsoft ensures that sub-contractors to whom Microsoft transfers our data enter into written agreements with Microsoft that are no less protective than terms of the OST.
27.	Is there a provision in the contract with the CSP which requires sub-contractors to notify the customer of any data breaches?	*The Cloud Guidance (pg.5) suggests a data user to ensure that the contract with a CSP obliges the CSP including its sub-contractors to notify the data user of any data breach.* Yes. As part of the OST, Microsoft ensures that sub-contractors to whom Microsoft transfers our data

Field Code Changed

No.	Question/requirement	Template response and guidance
		enter into written agreements with Microsoft that are no less protective than terms of the OST, which includes the requirement to notify us of any data breaches.
28.	Is there a provision in the CSP contract which require sub-contractors to provide any mechanism for timely handling in case of data breaches, such as to take speedy remedial action, to maintain business continuity, to meet legal obligations and to manage customer and public relations?	*The Cloud Guidance (pg.5) suggests that any mandatory notification by CSPs should facilitate timely handling of data breaches by data users and ensuring business continuity.* Yes. The OST states that Microsoft remains responsible for its sub-contractors' compliance with Microsoft's obligations in the OST, including in relation to any incident response obligations.
F. DIRECT MARKETING		
29.	What must the customer inform the data subject if the customer intends to use personal data in direct marketing? .	*"Direct Marketing" means the offering, or advertising of the availability, of goods, facilities or services or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes through sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication or making telephone calls to specific persons. Section 35C PDPO states that before a data user conducts direct marketing, the data user shall inform the data subject that the data user intends to use his/her personal data and may not use the personal data unless the data subject has given consent and the data user shall inform the data subject of the kinds of personal data that will be used and the classes of marketing subjects in relation to which data is to be used, and provide the data subject with a response channel to communicate his/her consent.* [ONLY If you will use personal data for direct marketing purpose] Yes. We have obtained the explicit consent of the data subject to use his/her personal data for direct marketing, where appropriate, as

No.	Question/requirement	Template response and guidance
		follows: • the following personal data will be used for directing marketing: [insert type of personal data e.g. contact details, age group]; and • the following classes of marketing subjects will be using the data subject's personal data: [insert marketing subjects e.g. cosmetic products, telecommunication network services]. We have also provided the data subject with the following response channels to provide his/her consent or withdraw his/her consent: [insert response channel e.g. a telephone hotline, a facsimile number, a designated email account, an online facility, a designated person to handle request from the data subject through the above or other means.] We have backed this up through our arrangements with Microsoft, since Microsoft will not use our data for purposes that are unrelated to providing the Microsoft cloud service such as for any advertising or similar commercial purposes.
G. TRANSFER OF DATA OUTSIDE HONG KONG		
30.	Will the locations/jurisdictions where the data will be stored by the CSP be disclosed to the customer?	*The Cloud Guidance (pg.3) suggests that a cloud provider should disclose to a data user the locations/jurisdictions of where data will be stored.* Microsoft discloses the geographical locations and regions of their data centers around the globe, in which our data is stored. Each Microsoft cloud service has its own location policies for customer data and such policies that contain the Geographical locations and Regions of our data are available at the Microsoft Trust Center.

Field Code Changed

No.	Question/requirement	Template response and guidance
31.	Will the locations/jurisdictions where the data will be stored by the CSP be chosen/ specified by the customer?	*The Cloud Guidance (pg.3) suggests that a data user should choose a CSP that allows the data user to specify locations/jurisdictions of where data will be stored.* Yes. Most Microsoft cloud services enable us to specify the locations/jurisdictions in which our data will be stored. Microsoft may replicate data within a selected geographical area for data durability but will not replicate or move customer data outside it. See the Microsoft Trust Center for more information on Microsoft Azure, Microsoft Office 365 and Microsoft Dynamics 365.
32.	Will the data storage location have adequate legal/regulatory privacy protection for personal data and judicial oversight over law enforcement agencies against arbitrary data access, including locations/jurisdictions outside Hong Kong?	*The Cloud Guidance (pg. 3) suggests that the data storage locations of a CSP should have adequate legal/regulatory personal data protection regime. For example, the regulatory regime of each data storage location of a CSP is substantially similar to the level of protection of personal data in Hong Kong.* Yes. Microsoft is committed to being transparent with the geographical locations and regions of its data centers, which are selected based on a detailed set of regulatory, political, socio-economic, geological and environmental factors and are published at the Microsoft Trust Center. Regarding requests for our data from law enforcement or other governmental entities, Microsoft is firm in its commitment to protect our data. Accordingly, Microsoft will not disclose our data to a third party (including law enforcement, other government entity or civil litigant) except as we direct or required by law. Should a third party contact Microsoft with a demand for our data, Microsoft will attempt to redirect the third party to request it directly from us. If Microsoft is compelled to disclose our data to a third party, they will promptly notify us and provide a copy of the demand, unless legally prohibited from doing so. Microsoft also publishes a Law Enforcement Requests Report that provides insight into the scope of requests, as well as information from Microsoft's General Counsel about how Microsoft responds to national security requests.

Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed
Field Code Changed

No.	Question/requirement	Template response and guidance
33.	Is there sufficiently clear and comprehensible notification to customers in their personal information collection statement and/or privacy policy statement that personal data processing may be outsourced to a CSP, that their personal data may be stored or processed in another jurisdiction, and that it may be accessible to law enforcement and national security authorities of that jurisdiction?	*The Cloud Guidance (pg.5) suggests that a data user must ensure that there is sufficiently clear notification to a data subject in its personal information collection statement and/or privacy statement that personal data processing may be outsourced to a CSP, and that the data subject's personal data may be stored in a separate jurisdiction which may be accessible to the authorities of that jurisdiction.* Yes, please refer to our Privacy Policy at [insert link] and personal information collection statement at [insert link].