8 Cloud Services

What responsibilities do organisations have under the PDPA when using cloud services to process personal data in the cloud?

8.1 When using cloud services, the organisation is responsible for complying with all obligations under the PDPA in respect of personal data processed by the cloud service provider ("CSP") on its behalf and for its purposes. Processing is defined in the PDPA as the carrying out of any operation or set of operations in relation to the personal data, and includes recording, holding, organising, adapting or altering, and retrieval of personal data.

What responsibilities do CSPs have under the PDPA for the personal data they process for organisations?

8.2 Where the CSP is processing personal data on behalf and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing, the CSP is considered a data intermediary and subject to the Protection and Retention Limitation Obligations under the PDPA. Its Protection and Retention Limitation Obligations extend to personal data that it processes or hosts for the organisation in data centres outside Singapore. The CSP, as an organisation in its own right, remains responsible for complying with all Data Protection Provisions in respect of its own activities which do not constitute processing of personal data under the contract. More information on the obligations of data intermediaries can be found in the Key Concepts Guidelines.

Who is responsible for complying with the Transfer Limitation Obligation for overseas transfers of personal data as part of CSPs' processing of personal data in the cloud?

8.3 An organisation that engages a CSP as a data intermediary to provide cloud services is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data in using the CSP's cloud services. This is regardless of whether the CSP is located in Singapore or overseas.

How should organisations ensure compliance with the Transfer Limitation Obligation for overseas transfers of personal data by their CSPs?

8.4 An organisation should ensure that any overseas transfer of personal data as a result of engaging a CSP will be done in accordance with the requirements under the PDPA, namely, the organisation could ensure that the CSP it uses only transfers data to locations with comparable data protection regimes, or has legally enforceable

obligations to ensure a comparable standard of protection for the transferred personal data. Such issues of compliance can be provided for in the written contract between an organisation and its CSP. The contract should deal with both the standard of protection and the overseas locations

8.5 The organisation may be considered to have taken appropriate measures to comply with the Transfer Limitation Obligation by ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients (e.g. data centres or sub-processors) in these locations are legally bound by similar contractual standards.

Example: Organisation ABC wishes to engage CSP DEF based in Singapore to process personal data in the cloud on its behalf. ABC had assessed that Hong Kong's data protection laws are comparable to the PDPA. Before signing up for its services, ABC conveys to DEF that it only wishes to store the personal data in data centres in Singapore and Hong Kong, and includes a clause in the contract to state so. A data breach subsequently occurs while the personal data is in the possession of DEF. ABC's due diligence in engaging DEF would be taken into consideration in the Commission's assessment of liability when determining whether ABC has breached its obligations under the PDPA. DEF may also be liable for breach of the Protection Obligation.
Example: Organisation GHI wishes to engage CSP JKL based in Singapore to process personal data in the cloud on its behalf. JKL will only store personal data in data centres in Singapore, Japan and South Korea. In engaging JKL's cloud services, GHI ensures that its contract with JKL specifies that the data centres and any sub-processors in Japan and South Korea are legally bound to comply with standards that are comparable to the PDPA. A data breach subsequently occurs while the personal data is in the possession of JKL. GHI's due diligence in engaging JKL would be taken into consideration in the Commission's assessment of liability when determining whether GHI has breached its obligations under the PDPA. JKL may also be liable for breach of the Protection Obligation.

8.6 CSPs based in Singapore have to meet the standards of protection under the Data Protection Provisions when they process personal data as data intermediaries. Industry standards like ISO27001 and Tier 3 of the Multi-Tiered Cloud Security

(MTCS) Certification Scheme could provide assurance of the CSP's ability to comply with the Protection Obligation of the PDPA.

8.7 Where the contract between an organisation and its CSP does not specify the locations to which a CSP may transfer the personal data processed and leaves it to the discretion of the CSP, the organisation may be considered to have taken appropriate steps to comply with the Transfer Limitation Obligation by ensuring that (a) the CSP based in Singapore is certified or accredited as meeting relevant industry standards, and (b) the CSP provides assurances that all the data centres or sub-processors in overseas locations that the personal data is transferred to comply with these standards. For example, the organisation could consider engaging a CSP that is certified as compliant with the ISO27001 standard and can produce technical audit reports such as the SOC-2 upon request.

Example:

Organisation MNO wishes to purchase an off-the-shelf cloud service offered by CSP PQR. In its standard end-user agreement, PQR does not specify the locations to which the personal data may be transferred in the course of processing. However, MNO ensures that all data centres and sub-processors to which personal data may be transferred to in using PQR's off-the-shelf cloud service are certified as compliant with the ISO27001.

A data breach subsequently occurs while the personal data is in the possession of PQR. MNO's due diligence in engaging PQR would be taken into consideration in the Commission's assessment of liability when determining whether MNO has breached its obligations under the PDPA. In particular, insofar as MNO has taken appropriate steps to ensure that PQR is able to comply with the PDPA in respect of the transferred personal data, MNO is taken to have satisfied the requirements for the Transfer Limitation Obligation. PQR may also be liable for breach of the Protection Obligation.

END OF DOCUMENT