20 The Accountability Obligation[38]

20.1 In data protection, the concept of accountability refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over[39]. This may include situations where the organisation can determine the purposes for which the personal data is collected, used or disclosed, or the manner and means by which the data is processed. This general concept of accountability is premised on section 11(2) of the PDPA, which states, "An organisation is responsible for personal data in its possession or under its control."

20.2 Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. Some of these measures are specifically required under the PDPA. For example, designating one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, developing and implementing policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("data protection policies and practices"), and making information about their data protection policies and practices available. Other measures as described at para 20.15 are not mandatory but are good practices to help organisations in meeting their obligations under the PDPA.

Appointing a Data Protection Officer

20.3 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as a data protection officer ("DPO"). Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that designation to another individual. Section 11(6) clarifies that the designation of an individual by an organisation under section 11(3) does not relieve the organisation of any of its obligations under the PDPA. That is, legal responsibility for complying with the PDPA remains with the organisation and is not transferred to the designated individual(s). On the whole, these provisions require organisations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, so that collectively,

[38] Previously known as the "Openness Obligation". This section has been updated to reflect developments in data protection relating to the concept of accountability as it applies to organisations which collect, use, disclose or process personal data, or control such collection, use, disclosure or processing.

[39] For more information, please refer to the PDPC's Guide to Accountability under the Personal Data Protection Act on the PDPC's website.

they co-operate to ensure that the organisation complies with the PDPA.

20.4 An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring and reporting data protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection. Depending on the organisation's needs, the DPO may also work with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions. The DPO can also play a role in supporting an organisation's innovation.

20.5 Individual(s) designated by an organisation under section 11(3) should be: (a) sufficiently skilled and knowledgeable; and (b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organisation. Organisations should ensure that individuals appointed as a DPO are trained and certified[40]. The individual(s) should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices. As part of corporate governance, the commitment and involvement of senior management is key to ensure that there is accountability and oversight over the management of personal data in the organisation.

20.6 The DPO (or someone working with him) may also be the primary contact point for the organisation's data protection matters. Section 11(5) of the PDPA requires an organisation to make available the business contact information of at least one individual designated by the organisation under section 11(3) while section 20(1)(c) and 20(4)(b) require an organisation to make available the business contact information of a person who is able to answer questions on behalf of the organisation relating to the collection, use or disclosure of personal data.[41] These

[40] For example, the Practitioner Certificate for Personal Data Protection (Singapore) co-issued by the PDPC and the International Association for Privacy Professionals ("IAPP").

[41] For the purpose of responding to access and correction requests in writing, at least one of the business contact information of this designated individual should be a mailing address (e.g. the office address) or an electronic mailing address.

individuals and persons may be the same individual or the organisation may have different persons undertaking such roles.

20.7 The business contact information of the relevant person should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

Developing and implementing data protection policies and practices

20.8 Section 12 of the PDPA sets out four additional key requirements which form part of the Accountability Obligation.

20.9 Firstly, an organisation is required to develop and implement data protection policies and practices to meet its obligations under the PDPA[42]. As part of this, organisations should develop both internal and external policies and practices (as required), taking into account matters such as the types and amount of personal data it collects, and the purposes for such collection.[43] This entails ensuring that policies and practices are easily accessible to the intended reader. The organisation should also put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices.

20.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA[44]. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts.

20.11 Thirdly, an organisation is required to communicate to its staff information about its policies and practices[45]. Such communication efforts could be incorporated in organisations' training and awareness programmes and should include any additional information which may be necessary for the organisation's staff to effectively implement its data protection policies and practices. An effective training

[42] See section 12(a) of the PDPA.

[43] See para. 20.15 for other measures an organisation may wish to adopt when developing its data protection policies and practices.

[44] See section 12(b) of the PDPA.

[45] See section 12(c) of the PDPA.

and awareness programme builds a staff culture that is sensitive and alert to data protection issues and concerns.

20.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint process[46]. This is to ensure that individuals are able to find the necessary information and, if necessary, have the means of raising any concerns or complaints to the organisation directly.

20.13 In general, an organisation's personal data protection policies and practices set the tone for the organisation's treatment of personal data, and provide clarity on the direction and manner in which an organisation manages personal data protection risks. These should be developed to address and suit specific business or organisational needs.

Other provisions related to the Accountability Obligation

20.14 The Data Protection Provisions also provide for specific circumstances where organisations have to be answerable to individuals and the PDPC, and be prepared to address these parties in an accountable manner. For example:

a) individuals may request for access to their personal data in the possession or under the control of an organisation, which enables them to find out which of their personal data may be held by an organisation and how it has been used;

b) individuals may submit a complaint to the Commission and the Commission may review or investigate an organisation's conduct and compliance with the PDPA[47];

c) the Commission may, if satisfied that an organisation has contravened the Data Protection Provisions, give directions to the organisation to ensure compliance including (amongst others) imposing a financial penalty of up to $1 million; and

d) individuals who suffer loss or damage directly as a result of a contravention of Parts IV, V or VI of the PDPA by an organisation may commence civil

[46] See section 12(d) of the PDPA.

[47] Sections 28 and 29 of the PDPA specify what the PDPA may do upon a review or investigation respectively.

proceedings against the organisation[48].

Other measures relating to accountability

20.15 Although not expressly provided for in the PDPA, organisations may wish to consider conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, and implementing a Data Protection Management Programme ("DPMP") to ensure that their handling of personal data is in compliance with the PDPA.[49] Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA. For example, an organisation that does not conduct a DPIA may not fully recognise risks to the personal data it is handling within its IT infrastructure. This, in turn, may result in the organisation failing to implement reasonable security measures to protect such data and hence committing a breach of section 24 of the PDPA.

Example:

In its effort to comply with the PDPA and demonstrate accountability, Organisation ABC undertakes a proactive and comprehensive approach by developing a DPMP. The DPMP incorporates data protection policies to provide transparency in the manner ABC handles personal data, processes as well as roles and responsibilities of the people in the organisation. As part of its corporate risk management framework, ABC also has in place a process to conduct DPIAs to identify, assess and address personal data protection risks.

Having implemented robust personal data protection policies and practices, ABC decides to certify its data protection policies and practices under the Data Protection Trustmark ("DPTM") Certification to enhance consumer trust and provide greater assurance for its stakeholders.

[48] Parts IV, V and VI of the PDPA relate respectively to (a) collection, use and disclosure of personal data; (b) access to and correction of personal data; and (c) care of personal data (containing provisions relating accuracy, protection, retention and transfer of personal data).

[49] For more information, please refer to the Guide to Data Protection Impact Assessments and Guide to Developing a Data Protection Management Programme on the PDPC's website.