UNDERSTANDING THE NEW REQUIREMENTS PERTAINING TO DATA PROTECTION OFFICERS IN SINGAPORE


OON THIAN SENG
FOUNDING PARTNER
HEAD OF CORPORATE

ANGELINE WOO
SENIOR ASSOCIATE

UNDERSTANDING THE NEW REQUIREMENTS PERTAINING TO DATA PROTECTION OFFICERS IN SINGAPORE

- Data protection is becoming increasingly important as organizations handle larger volumes of sensitive information in the digital age. With the rise of data breaches and stringent regulations like the Personal Data Protection Act 2012 ("PDPA"), safeguarding personal and business data is crucial to maintaining trust and legal compliance.

- Therefore, it is essential to employ a Data Protection Officer ("DPO") who specializes in monitoring data protection practices, ensuring regulatory adherence, and mitigating risks related to data privacy.

- The new requirement in Singapore regarding DPOs mandates that organisations in Singapore are required to file their DPO's business information with the Personal Data Protection Commission ("PDPC") via ACRA BizFile+ by 30 September 2024.

- An organisation must appoint one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. Nevertheless, the designation of an individual does not relieve the organisation of any of its obligations under the PDPA. Hence, the responsibility for complying with the PDPA remains with the organisation and is not transferred to the DPO.

- The business contact information of at least one DPO must be made available and according to the new requirement, this information must be filed on ACRA BizFile+. The business contact information must be easily accessible and operational during Singapore business hours. This contact information, which can be an email address, phone number, or other means of communication, should be accessible to the public, allowing individuals to easily reach the DPO. Therefore, in the case of telephone numbers, they must be Singapore-based telephone numbers. This is particularly crucial if the DPO is not physically based in Singapore, as it ensures the organisation can respond swiftly to the complaints or queries regarding its data protection policies and practices.

A: ORGANISATION'S ACCOUNTABILITY OBLIGATIONS UNDER THE PDPA

- The appointment of DPO(s) falls under organisations' "accountability obligation" which is one of the obligations that the data protection provisions under the PDPA impose on organisations with respect to their data activities.

- The appointment of DPO is mandatory as highlighted in the decision of ACL Construction (S) Pte Ltd; which underscored the necessity for organisations at the minimum, to appoint a data protection officer and establish protocols to ensure compliance with the PDPA. Pursuant to the obligation, an organisation must make reasonable efforts to ensure that the personal data it collects is accurate and complete, especially if it intends on using this data to make decisions that impact the individual concerned or plans to share it with another organisation. DPOs can be registered with the PDPC through its website, and the organisation must make the DPO's business contact information publicly available.

- Non-compliance with this requirement could result in a breach of the accountability obligations under the PDPA, potentially leading to penalties (a financial penalty up to a maximum of 10% of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher) or directions from the Personal Data Protection Commission (PDPC) to correct the issue.

B: WHO CAN BE APPOINTED AS DPO?

- The DPO role can either be a standalone position or added to an existing role in the organisation. For organisations with manpower constraints, outsourcing operational aspects of the DPO function to an external qualified firm is an option.

- Regarding the selection of a DPO, the PDPC has advised that the DPO should ideally be chosen from senior management and be sufficiently able to carry out their assigned responsibilities. If the DPO is not a C-level executive, they should have direct communication with the executive team. This access is essential to enable the DPO to effectively fulfil their role and responsibilities as the PDPC emphasised in Re M Stars Movers & Logistics Specialist Pte Ltd[1].

- In practice, it is recommended that an organisation appoint an individual (or team) knowledgeable about the data protection laws of Singapore, the organisation's data processing activities and data protection policies. This to enable the DPO to be capable of: (i) maintaining the organisation's compliance with the PDPA; (ii) addressing inquiries from authorities or the public regarding the organisation's data protection practices; and (iii) mitigating the effects of any data breach incidents.

C: RESPONSIBILITIES OF THE DPO

- Some of the non-exhaustive list of responsibilities of the DPO include;

- Developing and enforcing procedures and policies for managing personal data in line with your business's data protection responsibilities;
- Enhancing stakeholders' (eg. employees, independent contractors, and business partners) understanding of data protection policies and your organisation's data protection obligations in line with these polices;
- Addressing questions and complaints related to your business's handling of personal data; and
- Keeping management informed of potential data protection risks

D: HOW ORGANISATIONS CAN BENEFIT FROM OUTSOURCING THE DPO

- Therefore, given the level of responsibilities associated with the role of the DPO, outsourcing the DPO to a firm offers significant benefits. It ensures compliance, provision of expert guidance, and allows organisations to focus on their core business practice while maintaining high standards of data privacy and security.

- The benefits that the organisation would attain from outsourcing of the role are:

- Saving time, allowing the organisation to concentrate on its core operations.
- Fulfilling the independence requirements for the DPO role without affecting current internal responsibilities.
- Gaining access to expert consultants in cases of data breaches, regulatory investigations, or other privacy-related incidents who are highly attuned to industry trends and keep up with current legislation.

E: CONCLUSION

- In summary, data protection is becoming increasingly important with the rise of data breaches. Hence, it is essential to employ a DPO to mitigate risks relating to data privacy.

This article was authored by our Founding Partner Oon Thian Seng and Senior Associate Angeline Woo. The authors thank Trainee Aparna Sah for her valuable assistance with the article.

The ability to transfer customer data, employee files, financial records, and other information around the globe quickly and cheaply has opened up a world of opportunity for many businesses. It also presents a new world of risks and the need for businesses to consider how data is stored and managed. With the digital economy advancing at lightning speed, it is now more important than ever that data protection, privacy and cybersecurity issues are not ignored, and data storage and management are dealt with carefully.

At Oon & Bazul LLP, our lawyers advise on all aspects of data protection, privacy and cybersecurity, from helping you put the correct policies and procedures in place to helping you understand and ensure regulatory and legal compliance. Seamlessly working with their counterparts in other practice areas and specialist consultants, our lawyers provide integrated, creative and practical advice to our clients. We also have experience acting as a Data Protection Officer (DPO) for our clients.

You may visit our Data Protection, Privacy and Cybersecurity page to learn more about our practice.