Personal Data Protection in Singapore – Six Compliance Steps Every Singapore Business Should Take

December 2024

The Personal Data Protection Act 2012 ("PDPA") governs the collection, use and disclosure of personal data by organisations in Singapore. Despite the PDPA coming into full effect in 2014, data protection compliance remains a disregarded topic for many businesses. Yet, this negligence can easily become costly. Singapore's Personal Data Protection Commission ("PDPC") constantly takes action to enforce the law. For errant companies this often leads to considerable administrative effort in dealing with the authority, as well as to avoidable costs, penalties and reputational damage.

One of the reasons that Singapore companies may find it comparatively cumbersome to implement a data protection compliance programme could be that the respective requirements are not described in much detail in the PDPA itself. Specifics can rather be found only in the large number of advisory guidelines, practical guidance documents and decisions issued by the PDPC. This fragmentation of information sources makes it easy to lose track of what is important. It is therefore helpful to identify some straightforward steps that every Singapore business should take to establish its basic compliance framework. This can be done at manageable cost and will help to address the most common compliance gaps.

This overview aims to provide a clear and concise overview of six key compliance steps.

I.Preliminary consideration: What is personal data?

Personal data is, simply put, any information about human beings (such as employees, shareholders, directors, service providers, customers, business partners et cetera). Whether the information is true or not, is not relevant. If it allows the identification of the relevant person, possibly together with other information to which your organisation has or is likely to have access, the information is considered personal data.

A special category of personal data is business contact information ("BCI"). BCI refers to details such as a person's name, job title, work phone number, work address, work email, and work fax number, if they are provided (at least also) for professional purposes. The data protection provisions of the PDPA do generally not apply to BCI.

II.Six steps to compliance

Compliance Step 1: Appoint a data protection officer

Every Singapore organisation must designate at least one individual to be responsible for ensuring that it complies with the PDPA. This person is usually referred to as data protection officer ("DPO").

The responsibilities of the DPO are very broad. According to the PDPC, they "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."[1]

Companies should ensure that the person appointed as DPO is not only familiar with the PDPA, but also trained and certified. He may, for example, hold a certification issued by the International Association of Privacy Professionals ("IAPP").

Once a DPO is appointed, his BCI (or the BCI of another person to whom the respective responsibility is delegated) must be made available to the public. Your company secretary would usually handle this step via a filing with BizFile+, the business filing portal of the Singapore Accounting and Corporate Regulatory Authority.

Compliance Step 2: Set up a personal data inventory

Having an overview of your company's handling of personal data is the indispensable backbone of PDPA compliance. You need to be aware of the types of personal data your organisation collects, uses and/or discloses, for which purposes it does this, with whom it shares the personal data, when the personal data is disposed of, and so on.

[1] PDPC, Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 16 May 2022), p. 152.

Only then will your business be able to protect the relevant personal data appropriately and implement the necessary compliance measures.

Your DPO, together with the relevant operative business functions and the management of your company, should hence set up a personal data inventory, thus providing a comprehensive overview of your organisation's personal data processing activities.

Compliance Step 3: Review your personal data processing activities from a legal perspective

Once your personal data inventory is set up and your organisation's personal data processing activities are comprehensively documented, they should be reviewed from a legal perspective to ensure that they are in line with the PDPA's requirements. Where necessary, adjustments need to be implemented.

Compliance Step 4: Evaluate your sharing of personal data with third parties

Sharing personal data with third parties is a normal part of doing business. Whether the recipients are part of your group of companies or are independent third parties, whether you engage them to process personal data on your behalf (such as in the case of corporate service providers or online storage platforms) or you share the personal data with them so that they can use it for their own purposes, whether they are in Singapore or abroad: the PDPA sets out the requirements that must be met to ensure that the sharing of personal data is permitted. These requirements should be assessed, and the appropriate legal means put in place. Common examples are the implementation of data processing or data sharing agreements with the relevant third parties.

Compliance Step 5: Draft personal data protection policies

It is mandatory for organisations in Singapore to draft and implement the policies necessary to comply with the PDPA. Such policies are usually referred to as Personal Data Protection Policies ("PDP Policies"). In particular, an internal PDP Policy is intended to be a practical guide for your organisation's employees on how to handle personal data. It should address the findings of Compliance Steps 2 - 4 above and tell your employees and management what they can, should and must not do with respect to personal data. A PDP Policy should be tailored to your organisation's needs and processes, and should include or be accompanied by a data breach management plan that provides your organisation with a step-by-step plan for responding to a data breach.

Compliance Step 6: Implement your PDP Policies and train your staff

Even the best PDP Policy is only meaningful if it is implemented. To ensure that this happens, organisations have to train their staff on data protection issues. Information about the organisation's policies and practices should be clearly communicated. It is recommended to implement an effective training and awareness programme with regular updates and repetitions.

III. How we can support you

Gateway Law Corporation is well prepared to assist you with every step along your journey to PDPA compliance. We can especially provide the following support:

- provision of IAPP-certified personnel to act as external data protection officer for your business,
- set-up and maintenance of a personal data inventory,
- review of your organisation's personal data processing activities from a legal perspective,
- evaluation of your sharing of personal data with third parties and drafting the necessary agreements (e.g., data processing agreements, data sharing agreements, data transfer agreements),
- drafting other personal data protection-related documents, such as internal personal data protection policies, outside-facing privacy policies, notifications to employees and other individuals from whom your organisation collects personal data, and
- conducting training sessions for your staff and management.

Please do get in touch with us if you have any questions regarding your personal data protection compliance or our related services.

Your Contact

Sebastian Blasius

Attorney-at-law (Germany)
Foreign Lawyer (Singapore)
Certified Information Privacy Professional (Europe)
Certified Information Privacy Professional (Asia)

+65 89028272
sebastian.blasius@gateway-law.com

Sebastian Blasius has been practicing law in Singapore since 2015. He is among the select few German lawyers registered to practise not only foreign law, but also Singapore law (under the provisions of the Legal Profession Act 1966 and the rules made thereunder).

Throughout his career, Sebastian has advised organizations of all sizes and stages of development: from newly founded start-ups to established businesses, and from sole proprietorships to global corporations. He provides comprehensive counsel on all key areas of business law, particularly in corporate, employment, and general contract law.

Sebastian places a special focus on data protection law. Being an IAPP Certified Information Privacy Professional for Asia and Europe, Sebastian also acts as data protection officer for his clients. In addition, Sebastian regularly publishes insights on legal developments, or delivers lectures, seminars, and training courses on these subjects. Sebastian's publications on personal data protection and other topics are available for free download at the following link: https://gateway-law.com/sebastian-blasius/.

About Gateway

Gateway Law Corporation is a Singapore full service legal practice with strengths in the areas of intellectual property, franchising, technology, media (and entertainment), telecommunications, data protection and cybersecurity as well as employment and immigration. In addition to our niche areas, Gateway also provides services in the general areas of litigation and dispute resolution, corporate and commercial law, real estate conveyancing and advisory, medical law and family law.

Disclaimer