

Luther.

Personal Data Protection in Singapore – duties and obligations

Table of Contents

PDPA Compliance	3	Our PDPA Related Services	5
Your Obligations Under the PDPA	3	Audits	5
Collection / Processing / Retention	3	Policy Drafting	5
Security	3	Training	6
Transfer	4	Data Protection Officer	6
Marketing	4	Legal Advice Regarding Data Transfer	6
Online Privacy	4	Your Contact	6
Comprehensive Policy & Complaint Handling	4		
Data Protection Officer	5		



PDPA Compliance

Over recent years, data protection has become increasingly important for financial centres to stay competitive in a globalised economy. For this reason, Singapore has established the Personal Data Protection Act (“**PDPA**”), which was enacted in 2014. It comprises various rules governing the collection, use, disclosure and care of personal data. The PDPA contains two main sets of provisions which organisations are required to comply with. These cover, firstly, data protection in general and, secondly, the Do-Not-Call (“**DNC**”) registry.

The PDPA is intended to ensure a baseline standard of protection for personal data and complements sector-specific legislative and regulatory frameworks. The PDPA is, hence, not just a “recommendation” or “guideline” but has been accorded the force of law. In other words, organisations have to comply with the PDPA as well as the common law and other relevant laws, when handling personal data in their possession.

The first part of this brochure (A.) is to provide you with an overview on the Singaporean data protection regime. It may serve as an initial check-up for whether your organisation has implemented the necessary rules and policies to comply with the legislation on personal data protection.

In the second part (B.) we will explain in more detail how Luther LLP can assist you in complying with your PDPA related obligations.

A. Your Obligations Under the PDPA

The PDPA applies to all organisations carrying out activities involving personal data in Singapore irrespective of whether being registered in Singapore or not. Where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving personal data in Singapore.

I. Collection / Processing / Retention

The collecting and use of personal data by organisations is permitted only under certain conditions. Besides other obligations, the organisation is generally required to obtain the consent of the individual before collecting, using or disclosing his/her personal data. Further, an organisation may collect, use and/or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and of which the individual has been notified. Such notification must be made in accordance with the requirements of the PDPA.

Personal data should only be retained for as long as it is reasonable to assume that the purpose for which that personal data was collected no longer being served by retention of the personal data, and retention is no longer necessary for legal or business reasons.

It is further important to note that an individual may at any time withdraw any consent previously given or deemed to be given under the PDPA, upon giving reasonable notice to the relevant organisation.

II. Security

Organisations are obliged to protect personal data in their possession or under their control by making reasonable security arrangements in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar actions. The PDPA does not specify the exact security measures to have in place. This is left to the organisations. The Personal Data Protection Commission (“PDPC”) however may check if the existing measures in place are deemed sufficient and if not – for example, if any breach of the PDPA has endangered any personal data - may impose substantial penalties as prescribed by the PDPA. Organisations, therefore,

need to develop and implement their own security policies ensuring that the aforementioned minimum requirements are met.

III. Transfer

Transfer of personal data out of Singapore is allowed. However, it has to be ensured that the PDPA's standard of protection is accorded to this data. Hence organisations are, in general, required to ensure by way of contract/corporate rules/any other legally binding instrument that the personal data is protected in accordance with the PDPA. If no legal instrument is in place, the data may only be transferred to countries whose data protection laws have a standard comparable to the Singaporean one. This needs to be assessed on a case by case basis by comparing the relevant laws.

IV. Marketing

The data protection principles in the PDPA also apply to any marketing activities which involve the collection, use or disclosure of personal data. Moreover, electronic marketing activities are regulated under the Spam Control Act to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail, SMS and/or MMS to a mobile telephone number.

In addition to this, the PDPA contains specific complementary rules on marketing messages including both via text messages and phone calls. The Act applies to marketing messages addressed to a Singaporean telephone number where:

the sender of the marketing message is present in Singapore when the message is sent; or

the recipient of the marketing message is present in Singapore when the message is accessed.

Any organisation that wants to engage in telemarketing activities needs to comply with the "Do Not Call" provisions under the PDPA: Generally, an organisation intending to send marketing messages (including via phone calls and text messages) to a Singaporean telephone number should first obtain the clear and unambiguous consent of the individual. However, organisations may not require customers to give their consent to the sending of a specified message as a prerequisite for supplying goods, services, land, interest or opportunity beyond what is reasonable for the relevant supply.

In the absence of such consent it is necessary to check and ensure that the telephone number is not listed on the Do-Not-Call register maintained by the PDPC ("**DNC Register**"). An individual may at any time apply to the PDPC to add or remove his telephone number to or from the DNC Register.

In case the aforementioned prerequisites for sending a marketing message to a Singapore telephone number are fulfilled, the sender still needs to conform to the transparency requirements prescribed by the PDPA, that is, the sender must provide information allowing identifying and readily contacting the sender.

V. Online Privacy

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the PDPA. Nevertheless, an organisation that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the PDPA. For example, if an organisation intends to use cookies to collect personal data, it must obtain consent before the use of such cookies. For details regarding the consent required, please refer to the heading "Collection & Processing" above.

VI. Comprehensive Policy & Complaint Handling

Every organisation is further required by law to implement its own personal data protection policy. In this respect, a policy means a programme comprising structured internal processes and workflows in place to ensure compliance with the PDPA. While the law mandates only internal rules on how to deal with any personal data, it may be useful to have another one that is to be disclosed on request.

(This policy for disclosure explaining how the organisation treats personal data usually differ from the internal one in so far as it does not contain certain internal information that is not relevant or confidential. By contrast, the rights of members of the public in respect of their personal data are explained in much more detail.)

In addition, each organisation also needs to develop a process to receive and respond to complaints arising in connection with the collection, use or disclosure of personal data. Information on the complaint process has to be made available on request as well.

VII. Data Protection Officer

Each organisation is required to appoint at least one data protection officer (hereinafter also referred to as “DPO”) who is responsible for ensuring the organisation’s compliance with the PDPA. The DPO does not necessarily have to be an employee of the relevant organisation; an organisation is free to appoint whomever it deems fit to serve the purpose of ensuring its compliance with the PDPA.

However, failure to appoint a data protection officer may lead to a preliminary investigation by the PDPC. An organisation failing to cooperate and thereby impeding the investigations commits an offence. As a result, an organisation may be subject to a fine of up to SGD 100,000 (individuals may face a fine of up to SGD 10,000 or imprisonment for a term not exceeding 12 months).

Every organisation is required to publish the contact details of at least one data protection officer. While there is no requirement for the DPO to be a Singapore citizen or resident, the PDPC suggests that the data protection officer should be readily contactable from Singapore and available during Singaporean business hours. In cases where telephone numbers are provided these should be Singaporean numbers, too.

B. Our PDPA Related Services

Luther LLP is able to assist in ensuring full compliance with the PDPA. We offer a full range of legal services with respect to the PDPA. It is our goal to facilitate your daily work and minimise your compliance risks.

I. Audits

The first step of our comprehensive support and advice is a thorough two-stage audit of your organization. Such audit would provide us with a detailed picture of your organization’s personal data portfolio. The audit will help to detect any gaps and lapses in the organization’s data handling and it forms the basis for assessing the organization’s specific needs in developing a comprehensive personal data protection framework.

Usually we would, as a first step, provide you with the necessary documents to establish where personal data exists and how it is handled. Based on your information following the pre-audit, we would then, in a second step, conduct the actual audit consisting of an exhaustive review of the information collected, identification of potential compliance failures as well as a final report proposing the necessary amendments to the organisation’s personal data protection regime.

Our fees for the pre-audit documents are fixed at SGD 800 (SGD 936 with GST). The fees for the actual audit would have to be agreed on a case-by-case basis.

II. Policy Drafting

As mentioned, every organisation needs to have an adequate data protection policy in place. The policy needs to warrant the organisation complies with the PDPA requirements and especially safeguards the personal data in its possession.

Our fees for drafting such a policy depend on whether you merely need an internal policy (SGD 2,000, SGD 2,340 where GST applies) or a complementary external one, too (SGD 3,000 for both, SGD 3,510 where GST applies).

III. Training

We further offer training sessions to provide your data handlers with training in order to raise awareness of personal data protection and avoid future non-compliance. Fees vary according to our work involved and therefore would be agreed on a case-by-case basis.

IV. Data Protection Officer

1. DPO Services

As explained above, every organisation needs to have a DPO who is responsible for ensuring the organisation's compliance with the PDPA. As the DPO does not necessarily need to be an employee of the organisation, many organisations outsource the DPO function to PDPA specialists in order to ensure PDPA compliance as far as possible. The organisation thereby benefits from the knowledge and experience of the external DPO, enabling the organisations to have its own employees working on more business related matters. Luther LLP offers such a service at a monthly fee of SGD 350.

Please note that comprehensive knowledge about the personal data being handled by an organisation is a necessary requirement in order for a DPO to discharge his/her duties properly. Therefore, we can only act as an organisation's DPO where we have conducted the aforementioned audit and developed a policy prior to rendering our DPO services.

2. Data Protection Officer Nominee Services

In cases where we cannot offer our services as DPO because we have not conducted an audit and developed the policy, we can still offer our services to act as a so called Data Protection Officer Nominee ("DPO Nominee") for your organisation.

A DPO Nominee is a person engaged by the organisation to fulfil certain parts of the DPO's obligation.

The DPO Nominee provides publicly available contact details to which any requests and complaints about personal data can be sent to, inclusive of requests to amend or delete personal data.

Acting as a DPO Nominee, we undertake to provide our contact details to the public as well as to take note of any requests and to forward them to the person in charge at your organisation. We thus serve as a highly alerted and PDPA trained "mail box".

The advantage of our Nominee Services is that it ensures that any requests will be instantly attended to and forwarded to the right persons. As it has turned out in the past, high responsiveness is particularly important in case you receive complaints by the public and/or the PDPC.

For the Nominee Services, we charge a fixed monthly fee of SGD 100 (SGD 117 with GST). If a case should require subsequent advice, our usual hourly rates ranging between SGD 400 to SGD 600 (SGD 428 to SGD 642 with GST) apply.

V. Legal Advice Regarding Data Transfer

If you wish to transfer personal data abroad, we offer services that ensure the organisation abroad provides a standard of protection that is commensurate with the requirements prescribed under the PDPA. For legal advice in this respect, our fees will be charged on a time-cost basis at an hourly rate ranging between SGD 400 to SGD 600 (SGD 428 to SGD 642 with GST) depending on the seniority of the Attorney working on the matter.

Your Contact



Pascal Brinkmann LL.M. (Stellenbosch)

Rechtsanwalt / Attorney-at-Law (Germany)
Registered Foreign Lawyer (Singapore)
Phone: +65 6408 8000
Mobile: +65 9647 1977
Fax: +65 6408 8001
pascal.brinkmann@luther-lawfirm.com



Sebastian Blasius

Rechtsanwalt / Attorney-at-Law (Germany)
Registered Foreign Lawyer (Singapore)
Phone: +65 6408 8000
Mobile: +65 9489 4475
Fax: +65 6408 8001
sebastian.blasius@luther-lawfirm.com

[Disclaimer](#)

Although every effort has been made to offer current and correct information, this publication has been prepared to provide information on recent regulatory and legal developments in Singapore only. It is not exhaustive and thus does not cover all topics with which it deals. It will not be updated and cannot substitute individual legal and/or tax advice. This publication is distributed with the understanding that Luther LLP, the editors and authors cannot be held responsible for the results of any actions taken on the basis of information contained herein or omitted, nor for any errors or omissions in this regard.

Should you have any questions as to the PDPA and your obligations or should you like to explore any of the options covered in more detail, please do not hesitate to contact us.

Luther Rechtsanwaltsgesellschaft mbH advises in all areas of business law. Our clients include medium-sized companies and large corporations, as well as the public sector.

Berlin, Brussels, Cologne, Dusseldorf, Essen, Frankfurt a. M., Hamburg, Hanover, Leipzig,
London, Luxembourg, Munich, Shanghai, Singapore, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapore, Yangon

Your local contacts can be found on our website www.luther-lawfirm.com.



Hits the mark. Luther.

