GATEWAY LAW CORPORATION
Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

How To:

Get Started with your Data Protection Compliance Journey: Part 1

Overview

In this 4-part series of articles on getting started with a new business' data protection compliance journey, our Associate Director, Amira Budiyano sets out an easy to adopt formula and explores options that could suit most small and medium enterprises (SME) headquartered in or having a presence in Singapore.

In this first part, we discuss 2 beginning steps that any SME ought to take when starting out. It is presupposed that the reader has a basic understanding of the concept of personal data generally as well as the importance of protecting personal data.

The landscape today

Various countries around the world have pieces of legislations covering on protection of personal data and the corresponding penalties for failure to comply with such laws or regulations. In Singapore, the primary piece of legislation dealing with personal data protection is the Singapore Personal Data Protection Act 2012 which has been in effect since 2014. Non-compliance would result in being fined up to a maximum sum of SGD$1,000,000. At the time of this article, there has been at least 145 cases being decided by the Personal Data Protection Commission (PDPC) wherein a number of the cases relate to failure to put in place security arrangements and ensuring a standard of protection deemed acceptable. Whilst cyberattacks are more prevalent today, most of the cases dealt with data breaches arising not because of such attacks, but due to negligence and little prudence on the part of members of the organisation.

Step 1: Appointing a Data Protection Officer

It is interesting how in quite a number of the reported decisions, the penalised organisation has not appointed a data protection officer at all. Failure to fulfil this requirement tends to exacerbate the situation wherein a data breach has been found.

The PDPA only requires that an organisation one or more individual to be responsible for ensuring that the organisation complies with the PDPA. It is however possible for such individual to delegate said responsibility to another individual. Accordingly, the organisation has to make available to the public the business contact information of at least one individual appointed or designated. In any event, it is not such appointed or designated individual that will be under scrutiny or made to shoulder any burden of non-compliance; it is the organisation itself.

Appointing such individual(s), whom would be known as a "Data Protection Officer" need not be complicated nor strictly formal. Further, making available the requisite business contact information can be done by setting out on the organisation's website, or on social media.

GATEWAY LAW CORPORATION
Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Step 2: Preparing a Data Protection Policy

Preparing a "Data Protection Policy" is perhaps somewhat tricky for most businesses. In this respect, the PDPA requires that an organisation develops and implements policies and practices that are necessary for it to meet its obligations of the organisation under the PDPA as well as to develop a process to receive and respond to complaints that may arise accordingly. Further, staff needs to be communicated on its policies and practices, and these policies and practices must be made available on request.

This is where blindly adopting a model or sample policy would not work, especially if an organisation is not able to or does not wish to comply or adopt all of the implementations and measures described in said model or sample policy for various reasons. Imagine in a data breach investigation situation and the Data Protection Policy (wholly based on the sample) is being reviewed. It would not bode well for an organisation if it were to be found that the data breach could have been avoided if the organisation had adhered to the measures set out in such Data Protection Policy, as the impression given would be: rather that the organisation was unaware as to what it had to do to protect personal data or it was merely an unfortunate incident, it had actually failed, neglected or refused to implement what it said it would in its Data Protection Policy!

As you may have noticed as well, underlying this requirement of having a suitable Data Protection Policy would be to conduct training for staff. We will discuss more on such training in Part 2 of this *How To* series. For now, we focus on preparing a Data Protection Policy that works.

It is best to get a customised Data Protection Policy that fits *your* organisation, and a legal advisor would be able to help you with that. Minimally, a proper Data Protection Policy would contain the following information:-

- Introduction and objectives
- Type of personal data collected
- Consent and withdrawal of consent
- Purposes for which personal data is collected, used and/disclosed
- Personal data access, accuracy and correction
- Protection systems
- Storage and retention
- Complaint handling procedure
- Data Protection Officer

It is hoped that this Part 1 will encourage you to look at data protection compliance as something not to be feared. In the next Part, we will discuss the next strategies on how to get buy-in and acceptance from all members of your organisation.

Should you have any queries as to how this "How-to Guide" may affect your organisation or require further information, please do not hesitate to email us.

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Amira Nabila Budiyano
Associate Director
Gateway Law Corporation

Email: amira.budiyano@gateway-law.com

This article is intended to offer a systematic approach towards developing and implementing processes that could assist in data protection compliance with the Singapore PDPA but is not intended to be comprehensive nor should it be construed as legal advice.