Data Protection Governance Framework

30 Nov 2017

Document Control

Company	Prosec Services Pte Ltd
Title	Data Protection Governance Framework
Author	Al R Dizon, DPO
Filename	Prosec DP Governance Framework.docx
Owner	Al R Dizon, DPO
Subject	Data Protection Governance Framework
Review date	

Revision History

Revision Date	Revised by	Previous Version	Description of Revision

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contributors

- Management of Prosec Services Pte Ltd
- PDPA Committee of Prosec Services Pte Ltd
- Consultants from Straits Interactive Pte Ltd

Contents

This Data Protection Governance Framework lays down the organisation structure and framework for Prosec Services Pte Ltd ("Prosec" or "the Company") to manage the implementation of personal data protection policies and processes within the Company.

1 Background

The Singapore Personal Data Protection Act (PDPA) was passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012. The implementation of the Act was carried out in two stages:

- The Do-Not-Call (DNC) Provisions came into effect on 2nd January 2014; and
- The Personal Data Protection Provisions came into effect on 2nd July 2014. There are nine obligations under these provisions, namely
    - Consent
    - Purpose Limitation
    - Notification
    - Access and Correction
    - Accuracy
    - Protection
    - Retention Limitation
    - Transfer Limitation
    - Openness

    (See Appendix for details)

Where there is conflict between the PDPA and any sectoral law that is already in existence, the sectoral law will prevail.

2 Purpose

In order for Prosec to comply effectively with the requirements of the PDPA and to stay compliant over the long term, the Company needs a proper, institutional Data Protection Governance Framework.

The contents of this Governance Framework are elaborated in subsequent sections of this document.

3 Intended Audience

This Data Protection Governance Framework is applicable to:

- Prosec's Executive/Senior Management
- PDPA Committee
- Heads of Departments
- Data Protection Officer (DPO)

4 Scope

This Data Protection Governance Framework covers the following areas:

- Governance Principles
- Governance Structure with the roles and responsibilities of the major players
- Standardised Policies and Practices
- Standardised Processes and Mechanisms
- Common Enabling and Support Systems

5 Governance Principles

The following governance principles provide the guidance for the development and implementation of policies, practices, processes and systems to enable Prosec to comply with the PDPA and to stay compliant for the long term:

- PDPA compliance is not a one-time effort, but is a continual effort that has to be sustained for the long term.
- PDPA compliance is not a separate activity, but is to be an integral part of the business, operational and administrative processes of Prosec.
- PDPA compliance is the responsibility of everyone in Prosec, and not just the DPO.
- There must be clear definition of roles, responsibilities and accountabilities for the main players involved in Prosec's data protection programme.
- There should be standardised policies, practices, processes, mechanisms and systems for the implementation of the data protection programme in Prosec, as far as practicable.

6 Governance Structure

Sitting at the top of the governance structure is the PDPA Committee which comprises the key Heads of Departments who handle personal data in their day-to-day operations. The PDPA Committee provides the oversight over all data protection efforts in Prosec, sets the strategic directions and approves major programmes, initiatives and budgets. It also has overall accountability for the effective implementation of data protection policies and practices in Prosec.

The DPO, who is a member of the PDPA Committee, coordinates the data protection activities of the Company, including the formulation, implementation and updating of data protection and related policies and processes. The DPO is the external interface to the public, with his/her email address (**dpo@prosec.com.sg**) published on Prosec's website.

The Heads of Departments have accountability for ensuring and monitoring the effective implementation of data protection policies and practices that are embedded within the business, operational and administrative processes of their respective Department.

7 Standardised Policies and Practices

Prosec's objective is to have a set of standardised data protection policies and practices that is consistent across all Departments as far as practicable, unless unique business, operational or administrative requirements necessitate deviations from the standardised versions.

The DPO is responsible for promulgating the data protection policies and practices to all Departments so that all employees are aware of and understand:

- Prosec's principles, rules and guidelines on data protection;
- Their roles and responsibilities in complying with the policies and practices; and
- The consequences of their violating any of the rules.

Some of the above can be incorporated in the Employee's Handbook and Code of Conduct.

The policies will be reviewed and updated at least once every 24 months, or sooner (whenever there is a change or revision to the PDPA).

The following table identifies who within Prosec is Accountable, Responsible, Informed or Consulted with regards to the formulation, update and revision of the various data protection and related policies. The following definitions apply:

- **Accountable** – the person(s) with ultimate accountability and authority for the policy.
- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Accountable	PDPA Committee
Responsible	DPO, Heads of Departments
Consulted	IT Department, Legal Advisor
Informed	All Employees

Described below are the policies that are relevant to Prosec in order to comply with the nine obligations of the PDPA:

The **Internal Data Protection Policy** covers all the requirements under the nine obligations of the PDPA. Targeted at an internal audience, this Policy spells out the principles, guidance and processes of how Prosec handles the personal data of Employees, Members, Volunteers and Clients. It covers the collection, usage, disclosure, processing, analysis, protection, storage, retention and disposal of personal data in Prosec's possession or under Prosec control. All Prosec employees are required to comply with this Policy. The DPO is responsible for reviewing and updating this Policy periodically (once every 24 months) or as and when there is any change to the requirements of the PDPA.

The **Data Protection Notice/Statement** is targeted at the public at large. It fulfils the Openness Obligation of PDPA by informing the Data Subjects about Prosec's purpose of collecting, using and disclosing their personal data. The Notice/Statement also provides the business contact information of Prosec's DPO. It also contains instructions on how a member of the public can make an enquiry or complain to Prosec on data protection matters. The Data Protection Notice/Statement is posted on Prosec's website. The DPO is responsible for reviewing and updating this Notice/Statement periodically (once every 12 months) or as and when there is any change to the requirements of the PDPA.

Complementing the Internal Data Protection Policy is the **Information Security Policy** as "there is no privacy without security". The Information Security Policy spells out the preventive security measures to protect personnel data of Prosec employees against unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks. This Policy fulfils the Protection Obligation of the PDPA. All Prosec employees are required to comply with this Policy. The DPO, together with the IT Department, is responsible for reviewing and updating this Policy periodically (once every 24 months) or as and when there is a need to modify existing security measures or implement new ones.

The **Information Security Policy** includes a set of policies on terms of use governing computing devices or accompanying media owned by Prosec employees. This is known as the **Bring-Your-Own-Device Policy,** or BYOD Policy. Only when approved and registered by the IT Department may these devices or accompanying media be used to access Prosec's networks, application systems and databases within or outside the standard working hours. The IT Department is responsible for reviewing and updating this Policy (once every 12 months) or as and when there is a need to amend or update the terms of use.

The **Document Retention Policy** specifies the retention period of various classes of personal data and types of documents maintained by Prosec. It fulfils the Retention Limitation Obligation of the PDPA that requires these data or documents to be disposed of or destroyed once there is no longer any business or legal/statutory purpose for retaining them. Departments that hold these data and documents are required to abide by the retention schedules in this Policy. The DPO is responsible for reviewing and updating this Policy (once every 12 months) or as and when there is change in PDPA requirements. Each Department is responsible for reviewing and updating their retention schedules,

and for disposing/destroying their own personal data or documents (both in paper and electronic forms) that have reached the end of the retention periods.

The **Social Media Policy** specifies and explains the rules governing the use of social media in the Company. It also covers the rules pertaining to the use of social media during working hours and what can or cannot be posted on social media about Prosec or Company-related matters and issues. The DPO, together with the IT Department, is responsible for reviewing and updating this Policy periodically (once every 12 months) or as and when there is a need to modify existing terms and conditions of use.

8 Standardised Processes and Mechanisms

Prosec's objective is to have a set of standardised data protection processes and mechanisms that is consistent across all Departments as far as practicable, unless unique business, operational or administrative requirements necessitate deviations from the standardised versions.

Described below are the main data protection processes and mechanisms in Prosec that can be standardised.

8.1 Maintaining Personal Data Inventory and Data Flows

Prosec's personal data inventory and data flows are developed from the bottom-up by the various Departments. These provide a holistic view of the data items that are collected, used, disclosed and maintained by each Department and how they flow within the Company and with external parties outside the Company. All these separate inventories are integrated into a single corporate view so that there is clear visibility of the entire body of personal data that is in the possession of Prosec.

Each Department is responsible for maintaining and updating its own data inventory and data flows.

8.2 Maintaining Risk Register

Every Department in Prosec that needs to handle personal data in its business functions and operations has to maintain a register of data protection risks identified in the collection, use, disclosure and storage of personal data. The risk register will also include the measures and controls taken or are being planned to mitigate the risks. The effectiveness of such measures and controls have to be monitored or modified as necessary.

Each Department is responsible for maintaining and updating its own risk register and the progress made in implementing the measures and controls.

8.3 Maintaining Training and Awareness Programme

All employees must be kept abreast of the most current data protection policies and practices of Prosec, through continual training and awareness sessions. The training and awareness materials have to be standardised across Prosec so that all employees receive the same, consistent content and communication messages. Likewise, the

Employee's Handbook and Code of Conduct have to be updated with the most current data protection policies and practices.

The DPO, together with HR Department, is responsible for maintaining and updating the training and awareness materials.

HR Department is responsible for maintaining and updating the Employee's Handbook and Code of Conduct.

8.4 Using Consent Clauses

As far as practicable, consent clauses for obtaining consent from data subjects before collecting their personal data (via physical forms or electronic forms) will be standardised, with some variations in the wordings to suit different business areas. Related to this, clauses for withdrawal of consent or for opt-in / opt-out will also be standardised, again allowing for variations for different business areas.

The DPO (with appropriate legal advice as necessary) is responsible for reviewing and updating these clauses. The revised and updated clauses will be approved by the DPO before they are released for adoption by all Departments.

8.5 Maintaining Master Withdrawal List

Data subjects can withdraw their consent at any time by

- writing in to Prosec;
- selecting the "UNSUB" option of an online service; or
- invoking the "opt-out" clause in an existing agreement.

Their point of contact could be the Department that is serving them, the DPO whose name appears in the Prosec website, or the feedback channel on the website. The relevant Department will be responsible for handling the request and entering the data subjects' names into a Master Withdrawal List to be shared across all Departments. This is to inform everyone in Prosec with a 'need to know' that these individuals have withdrawn their consent and their personal data should no longer be used.

IT Department is responsible for maintaining the Master Withdrawal List and keeping it current.

8.6 Handling Access and Correction Requests

Any data subject may approach Prosec at any time to request access to and, if necessary, correction of their personal data held by Prosec. Their point of contact could be the Department that is serving them, the DPO whose name appears in the Prosec website, or the feedback channel on the website. The relevant Department will be responsible for handling the request. The staff in that Department will first authenticate the identity of the requester before processing the request within the stipulated period (i.e. 30 days as specified in the Personal Data Protection Regulations 2014). If the request cannot be processed within 30 days, the DPO will have to be informed. The DPO will then write to the requester to inform him/her about the time extension needed. The DPO may also inform the requester of the fee chargeable for processing his/her request.

Finance Department is responsible for working out an administrative fee structure that is standardised across Prosec.

Every access and correction request must be logged and tracked by the Department responsible until closure. An IT-based system can help to manage the logging and tracking. *(See Section 9).*

8.7 Retaining Data and Documents

All Departments will follow standardised data and document retention schedules for common classes of data or common types of documents, based on Prosec's business and legal requirements. Those data and documents that have statutory requirements (e.g. ACRA, MAS, IRAS) will abide by the mandated statutory periods of retention. All other data or documents that are unique to each Department will adopt their own retention schedules. *(Refer to the **Document Retention Policy** for more details).*

Heads of Departments will be responsible for monitoring the retention periods of the data and documents under their care, and to dispose/destroy them securely when they are no longer needed.

8.8 Managing Third-Parties and Data Intermediaries

When personal data in the possession of Prosec is disclosed to external third-parties or data intermediaries, there should be indemnity clauses in the contracts or agreements to indemnify Prosec against any loss or misuse of the personal data. Alternatively, a letter of undertaking could be used, instead of the more onerous indemnity clauses, when the circumstances warrant it (e.g. where the risk of exposure is assessed to be low). The external third-parties or data intermediaries are not allowed to further disclose the personal data to other parties unless there are clear specifications in the indemnity clauses or letters of undertaking.

The text in the indemnity clauses and letter of undertaking will be standardised as far as practicable. The DPO (with appropriate legal advice as necessary) is responsible for drafting, reviewing and updating these clauses and text. The revised and updated clauses and text will be approved by the DPO before they are released for adoption by all Departments.

8.9 Transferring Data Outside Singapore

Personal data in the possession of Prosec may be transferred to third-parties or data intermediaries outside Singapore. There should be appropriate clauses in the contracts/agreements or letters of undertaking with these organisations to specify the data protection requirements that are at least of the same standard as Singapore's PDPA. The external third-parties or data intermediaries are not allowed to further disclose the personal data to other parties unless it its clearly stated in the indemnity clauses or letters of undertaking.

The DPO (with appropriate legal advice as necessary) is responsible for drafting, reviewing and updating the clauses and text. The revised and updated clauses and text will be approved by the DPO before they are released for adoption by all Departments.

8.10 Handling Feedback and Complaints

Any data subject, or member of the public, may feed back to Prosec or make a complaint on matters related to data protection in Prosec. Their point of contact could be the Department that is serving them, the DPO whose name appears in the Prosec website, or the feedback channel on the website. Depending on the nature of the feedback or complaint, the relevant Department will be responsible for handling the case. If the magnitude of the feedback or complaint is beyond the authority or competence of the Department to handle, then the case will be escalated to the DPO or even the PDPA Committee.

The DPO must be alerted immediately if the feedback or complaint involves a data breach or data loss. Depending on the severity of the data breach or data loss, the DPO may decide to notify the data subjects affected or even the Personal Data Protection Commission (PDPC).

Every feedback or complaint must be logged and tracked by the Department responsible until closure. An IT-based system can help to manage the logging and tracking. *(See Section 9).*

8.11 Handling Incidents

No matter how much precaution and preventive measures are taken by Prosec to prevent incidents from happening, incidents affecting personal data protection often come unannounced. Depending on the nature of the incident, the affected Department may draw upon expertise from other Departments e.g. IT Department. If the magnitude of the incident is beyond the competence of the Department and other in-house expertise to deal with, the incident will be escalated to the DPO or even the PDPA Committee.

The DPO must be alerted immediately if the incident involves a data breach or data loss. Depending on the severity of the data breach or data loss, the DPO may decide to notify the data subjects affected or even the Personal Data Protection Commission (PDPC).

Every incident must be logged and tracked by the Department responsible until closure. An IT-based system can help to manage the logging and tracking. *(See Section 9).*

8.12 Conducting Periodic Onsite Audits

Onsite audits will be carried out by all Departments at least once a year to ensure that all employees abide by Prosec's policies, practices and processes pertaining to personal data protection and information security. The findings of the onsite audits and the corrective or remedial measures taken must be logged and tracked by the Department responsible until closure. An IT-based system can help to manage the logging and tracking. *(See Section 9).*

9 Common Enabling and Supporting Systems

Prosec will have a common IT-based system in place to manage and monitor the many data protection activities in the data protection programme in order to have a sustainable long-term compliance of the PDPA. These are:

- A system with a whole suite of capabilities (such as Straits Interactive's Data Protection Management System (DPMS)) to allow all Departments to:
    - update the compliance dashboards and track the progress of action plans;
    - maintain and update the personal data inventory and data flows;
    - perform in-house audits of data protection processes and practices;
    - monitor and track the control measures to mitigate data protection risks;
    - monitor and track data protection training programmes;
    - monitor and track communication and awareness campaigns on data protection;
    - monitor and track requests for access and correction to personal data and the follow-up actions;
    - monitor and track feedback and complaints related to data protection and the follow-up actions; and
    - monitor and track incidents related to data protection and the follow-up actions.

- A Master Withdrawal List of data subjects who have withdrawn their consent by
    - writing in to Prosec;
    - selecting the "UNSUB" option of an online service; or
    - invoking the "opt-out" clause in an existing agreement.

10 Review and Revision

This Data Protection Governance Framework will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

The review will be undertaken by the DPO in conjunction with the relevant Departments.

Approval and Effective Date: 30/11/17

Approved by: _____ Date: 30/12/17

Name: Rene M Shepherdson JR, PBM

Designation: GM/DIRECTOR, Prosec Services Pte Ltd

Prepared by:

Data Protection Officer

Name: AL R DIZON

Email: dpo@prosegur-prosec.sg

APPENDIX – Nine Obligations of PDPA 2012

In compliance with the PDPA, any Organisation that is collecting, using or disclosing personal data has to abide by the following requirements *(Section 11 of PDPA 2012):*

"(1) In meeting its responsibilities under this Act, an Organisation shall consider what a reasonable person would consider appropriate in the circumstances.
(2) An Organisation is responsible for personal data in its possession or under its control.
(3) An Organisation shall designate one or more individuals to be responsible for ensuring that the Organisation complies with this Act.
(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation.
(5) An Organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4).
(6) The designation of an individual by an Organisation under subsection (3) shall not relieve the Organisation of any of its obligations under this Act."

In addition, under *Section 12 of PDPA 2012*, the Organisation has to put in place the following policies and practices:

"An Organisation shall —
(a) develop and implement policies and practices that are necessary for the Organisation to meet the obligations of the Organisation under this Act;
(b) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;
(c) communicate to its staff information about the Organisation's policies and practices referred to in paragraph (a); and
(d) make information available on request about —
(i) the policies and practices referred to in paragraph (a); and
(ii) the complaint process referred to in paragraph (b)."

Consent (Section 13)
"An Organisation shall not, on or after the appointed day [2 July 2014], collect, use or disclose personal data about an individual unless —
(a) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or
(b) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law."

Purpose Limitation (Section 18)
"An Organisation may collect, use or disclose personal data about an individual only for purposes —
(a) that a reasonable person would consider appropriate in the circumstances; and
(b) that the individual has been informed of under section 20, if applicable."

Notification (Section 20(1))
"An Organisation shall inform the individual of —

(a) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data;
(b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (a), before the use or disclosure of the personal data for that purpose; and
(c) on request by the individual, the business contact information of a person who is able to answer on behalf of the Organisation the individual's questions about the collection, use or disclosure of the personal data."

Access and Correction (Section 21(1), Section 22(1))
"On request of an individual, an Organisation shall, as soon as reasonably possible, provide the individual with —
(a) personal data about the individual that is in the possession or under the control of the Organisation; and
(b) information about the ways in which the personal data referred to in paragraph(a) has been or may have been used or disclosed by the Organisation within a year before the date of the request."

"An individual may request an Organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the Organisation."

Accuracy (Section 23)
"An Organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the Organisation is accurate and complete, if the personal data —
(a) is likely to be used by the Organisation to make a decision that affects the individual to whom the personal data relates; or
(b) is likely to be disclosed by the Organisation to another Organisation."

Protection (Section 24)
"An Organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks."

Retention Limitation (Section 25)
"An Organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —
(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and
(b) retention is no longer necessary for legal or business purposes."

Transfer Limitation (Section 26(1))
"An Organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that Organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act."

Openness (Section 11)
"(1) In meeting its responsibilities under this Act, an Organisation shall consider what a reasonable person would consider appropriate in the circumstances.
(2) An Organisation is responsible for personal data in its possession or under its control.
(3) An Organisation shall designate one or more individuals to be responsible for ensuring that the Organisation complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation.

(5) An Organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4).

(6) The designation of an individual by an Organisation under subsection (3) shall not relieve the Organisation of any of its obligations under this Act."