UPDATES TO THE PERSONAL DATA PROTECTION ACT 2020

*On 2 November 2020, amendments to the Personal Data Protection Act ("**PDPA**") were introduced to strengthen consumer protection while supporting the legitimate use of personal data by businesses, especially for purposes of growth and innovation. While businesses have to brace themselves for stiffer penalties in respect of data breaches, more opportunities are also afforded to businesses for legitimate uses of personal data.*

The Personal Data Protection (Amendment) Bill ("**Bill"**) was passed in Parliament on 2 November 2020, which seeks to amend the PDPA to strengthen the accountability of organisations by enhancing the legal framework for the collection, use and disclosure of personal data. This includes enhancing the enforcement powers of the Personal Data Protection Commission ("**PDPC**"), as well as providing individuals with greater autonomy over their personal data. Organisations can expect **an increase in the compliance requirements for personal data protection.**

ACCOUNTABILITY OBLIGATIONS

One of the amendments introduced under the Bill is to make explicit the accountability obligations owed by organisations, which are set out in sections 11 and 12 of the PDPA.

Section 11(3) of the PDPA requires an organisation to appoint a data protection officer ("**DPO**") who will be responsible for ensuring that the organisation complies with the PDPA. Some of their responsibilities include:

- Ensuring compliance with the PDPA when developing and implementing polices and processes for handling personal data;
- Monitoring and reporting data protection risks to the management team;
- Fostering a data protection culture and accountability among employees and communicating personal data protection policies to stakeholders;
- Handling and managing personal data protection related queries and complaints from the public; and
- Liaising with the PDPC on data protection matters, if necessary.

Section 12 also requires the organisation to do the following:

- Develop and implement data protection policies and practices by considering the types and amount of personal data collected, and the purpose of such collection;
- Develop a process to receive and respond to complaints in respect of the organisation's personal data protection polices and processes;
- Train and communicate to its staff about the organisation's PDPA policies and practices; and
- Make information on its data protection polices and practices and its complaint process available on request.

While it is not expressly provided for in the PDPA, it is recommended that organisations implement a Data Protection Management Programme ("**DPMP**") to ensure their handling of personal data complies with the PDPA.

Organisations should also consider conducting Data Protection Impact Assessments ("**DPIA"**) when they are introducing or developing a new IT system or process that involves the collection, use and/or storage of personal data. By failing to conduct DPIA, organisations may not know what reasonable security arrangements should be implemented to protect its personal data, thereby breaching section 24 of the PDPA.

> At the very basic level, **an appropriate data protection policy should be drafted to ensure that it gives a clear understanding within the organisation of its obligations under the PDPA and sets general standards on the handling of personal data which staff are expected to adhere to**.
>
> To meet these aims, the framers, in developing such policies, have to address their minds to the types of data the organisation handles which may constitute personal data; the manner in, and the purposes for, which it collects, uses and discloses personal data; the parties to, and the circumstances in, which it discloses personal data; and the data protection standards the organisation needs to adopt to meet its obligations under the PDPA.
>
> *Re M Star Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15 (at [25])

A case in point is that involving Horizon Fast Ferry Pte. Ltd. [2019] SGPDPC 27, which had engaged an independent contractor to revamp its booking site back in May 2017. Unknown to the organisation, the independent contractor replicated the auto-retrieval and auto-population feature in the revamped booking site, which enabled the system to automatically retrieve and populate the fields in the booking form with the user's passport number.

The PDPC found that the material time of the incident, Horizon Fast Ferry did not have a DPO, and it only implemented and uploaded its privacy policy after the incident. Further thereto, the organisation did not conduct any proper user acceptance tests before launching the revamped booking site. Unfortunately, this allowed for the unauthorised access to personal data to go undetected. As a result, Horizon Fast Ferry was directed to pay a financial penalty of $54,000.

MANDATORY DATA BREACH NOTIFICATION

Under the new amendments, organisations will also be required to notify the affected individuals as well as the PDPC in the event of a data breach where:

- Data breach is likely to result in **significant harm** – this would generally involve personal data such as:

  (1) The individual's full name or NRIC **in combination** with his personal data that are not publicly disclosed such as financial information; life/health insurance information; and private key used to authenticate or sign an electronic record or transaction.

  (2) The Individual's account information **in combination** with any codes or passwords used to permit access to or use the account.

- Where the data breach affects **500 or more individuals** even if the data breach does not involve the prescribed types of personal data as set out above.

Once it is determined that the data breach is notifiable, the organisation must notify the PDPC no later than three (3) calendar days after the data breach, and **where required**, the affected individuals as soon as practicable, at the same time or after notifying the PDPC.

Individuals need **NOT** be notified of the data breach if:

- An organisation has taken timely remedial action that renders it unlikely that the data breach will result in significant harm to the affected individuals; or

- Technological measures (e.g. encryption, password-protection, etc.) are applied before the data breach occurred, which renders the personal data inaccessible or unintelligible to an unauthorised party.

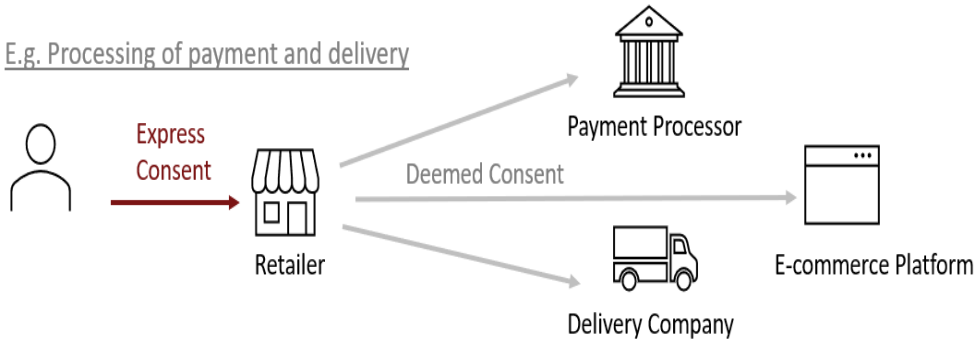
EXPANDED SCOPE OF "DEEMED CONSENT"

The amendments have also expanded the scope of "deemed consent" to include:

- Deemed consent by contractual necessity under the new section 15(3) of the PDPA; and
- Deemed consent by notification under the new section 15A of the PDPA.

Contractual Necessity

Consent is deemed where an individual provides his personal data to one organisation for the purpose of a transaction, and it is **reasonably necessary** for the said organisation to disclose to other organisations downstream for the completion of the relevant transaction.



Notification

In situations where an organisation wishes to use or disclose existing data for **secondary purposes** that are different from the primary purposes for which it had originally collected the personal data, an individual may be deemed to have consented to the collection, use, or disclosure of his personal data for the secondary purpose **if he had been notified of, and has not taken any action to opt out of it.**

Organisations seeking to rely on deemed consent by notification needs to do the following:

- Conduct an assessment to eliminate or mitigate adverse effects on the individual;
- Take reasonable steps to ensure that notification provided to individuals is adequate; and
- Provide a reasonable opt-out period.

NEW CONSENT EXCEPTIONS

Section 17 of the PDPA permits the collection, use, and disclosure of personal data without consent only in the circumstances set out in the new First and Second Schedules to the PDPA.

Legitimate Exception

The PDPA provides that an organisation may rely on the "legitimate interests" exception to collect, use, and disclose personal data without consent where the **legitimate interest outweighs any adverse effect on the individual**.

Organisations must therefore conduct an assessment to identify any potential adverse effect, and develop reasonable measures to eliminate, reduce the likelihood of, or mitigate the adverse effect on the individual. They must also take reasonable steps to provide the individual with reasonable access to information for which they are seeking to rely on the exception.

Examples of legitimate interests include the detection and prevention of illegal activities or threats to physical safety, IT and network security; preventing misuse of services; carrying out necessary corporate due diligence etc.

Business Improvement Exception

Organisations are allowed to **use**, without consent, personal data that they had collected, where the utilisation of personal data helps to achieve the following business improvement purposes:

- Improving, enhancing, or developing new goods and services or new methods or processes;
- Learning or understanding behaviour and preferences of individuals; or
- Identifying goods or services that may be suitable for individuals or personalising or customising any such goods or services for individuals.

In relying on the "business improvement" exception, organisations need to ensure that:

- The business improvement purposes **cannot be achieved without using the personal data in an individually identifiable form**;
- The use of data is considered **appropriate by a reasonable person**; and
- The data is not used for purpose of sending direct marketing messages.

An example where the "business improvement" exception would apply would be the use of personal data to train machine learning models.

For instance, a wearables company intend to use personal data of customers (i.e. heart rate, steps count) to train its machine learning model for monitoring of vital signs and develop new functionality. The company can rely on the "business improvement" exception to use their customers' personal data without consent to improve or personalise its goods or services if historical personal data is necessary when personalising new product features for its respective customers.

ENHANCED PENALTIES FOR MISHANDLING OF PERSONAL DATA

Apart from increasing the maximum financial penalty for PDPA breaches to 10% of an organisation's annual turnover in Singapore or S$1m, whichever is higher, the Bill will introduced personal liability for individuals who are found to have egregiously mishandled personal data by way of:

- Knowing or reckless unauthorised disclosure of personal data;
- Knowing or reckless unauthorised use of personal data for a gain or to cause a harm or loss to another person; and
- Knowing or reckless unauthorised re-identification of anonymised data.

The **introduction of new personal liability offences, however, does not detract from the existing position of holding organisations primarily accountable for data protection**.

Section 53 states that organisations remain liable for the actions of their employees in the course of their employment with the organisations. Depending on the terms of the service contracts or written agreement, organisations may also be liable for its service providers which they have engaged and authorised to process its personal data. It is therefore important to incorporate personal data protection clauses into the respective service contracts or written agreements.

Data Intermediaries

In the case of Horizon Fast Ferry Pte. Ltd. [2019] SGPDPC 27, Horizon Fast Ferry did not enter into any written agreement with the independent contractor engaged to revamp its booking site. Neither was there any evidence to suggest that the contractor stored, held, or managed the personal data on behalf of the organisation. Accordingly, the PDPC found that the contractor is not a data intermediary, and the Horizon Fast Ferry is solely responsible for complying with the PDPA, including the obligation to make reasonable security arrangements to protect the personal data under section 24 of the PDPA (see [22]).

In contrast, the PDPC in AIG Asia Pacific Insurance Pte Ltd & Toppan Forms (S) Pte Ltd [2019] SGPDPC 2 found that AIG's printer vendor Toppan Forms was a data intermediary for AIG as it would have to process the personal data on AIG's behalf to provide printing, collation and delivery services for AIG. Notwithstanding the following, under section 24 of the PDPA, AIG owed the same obligation in respect of personal data processed by Toppan as if the personal data were processed itself.

With regard to Toppan mailing out 87 policy renewal letters to the wrong addressee, the PDPC found that AIG did not breach section 24 of the PDPA. In making such a determination, the PDPC noted that AIG had included personal data protection covenants in its contract with Toppan, in particular (see [36]):

- That Toppan is to inform itself regarding, and comply with, AIG's privacy policies and all applicable privacy laws; and
- That Toppan is to maintain adequate administrative, technical and physical safeguards to ensure the security and confidentiality of the AIG's personal data, protect against any anticipated threats or hazards to the security or integrity of the personal data, and protect against unauthorised access to, use of or disclosure of personal data.

Therefore, the importance of incorporating personal data protection covenants in the contractual agreements with service providers and/or vendors that handle the organisation's personal data cannot be overstated.

At **Infinity Legal LLC**, our PDPA Practice, comprising lawyers who are Certified Personal Data Practitioners, aims to provide your organisation with a holistic, yet practical approach to complying with the PDPA. We help clients navigate through the variety of legal issues involving personal data protection

CONTACT US

INFINITY LEGAL LLC
无限法律事务所

6 Eu Tong Sen Street
#12-14 The Central
Singapore 059817

www.infinitylegal.com.sg

T: +65 6988 8986
F: +65 6988 8932
E: enquiry@infinitylegal.com.sg