Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy 2022

Singapore: Law & Practice
and
Singapore: Trends & Developments

Tat Lim and Chiew Khoon Heng
Aequitas Law LLP

practiceguides.chambers.com

SINGAPORE

Law and Practice

Contributed by:
Tat Lim and Chiew Khoon Heng
Aequitas Law LLP see p.21

CONTENTS

1. Basic National Regime p.3
1.1 Laws p.3
1.2 Regulators p.4
1.3 Administration and Enforcement Process p.5
1.4 Multilateral and Subnational Issues p.6
1.5 Major NGOs and Self-Regulatory Organisations p.7
1.6 System Characteristics p.7
1.7 Key Developments p.7
1.8 Significant Pending Changes, Hot Topics and Issues p.9

2. Fundamental Laws p.9
2.1 Omnibus Laws and General Requirements p.9
2.2 Sectoral and Special Issues p.12
2.3 Online Marketing p.14
2.4 Workplace Privacy p.14
2.5 Enforcement and Litigation p.14

3. Law Enforcement and National Security Access and Surveillance p.15
3.1 Laws and Standards for Access to Data for Serious Crimes p.15
3.2 Laws and Standards for Access to Data for National Security Purposes p.15
3.3 Invoking Foreign Government Obligations p.15
3.4 Key Privacy Issues, Conflicts and Public Debates p.15

4. International Considerations p.16
4.1 Restrictions on International Data Issues p.16
4.2 Mechanisms or Derogations that Apply to International Data Transfers p.16
4.3 Government Notifications and Approvals p.16
4.4 Data Localisation Requirements p.16
4.5 Sharing Technical Details p.17
4.6 Limitations and Considerations p.17
4.7 "Blocking" Statutes p.17

5. Emerging Digital and Technology Issues p.17
5.1 Addressing Current Issues in Law p.17
5.2 "Digital Governance" or Fair Data Practice Review Boards p.19
5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation. p.19
5.4 Due Diligence p.19
5.5 Public Disclosure p.20
5.6 Other Significant Issues p.20

1. BASIC NATIONAL REGIME

1.1 Laws

Singapore's Personal Data Protection Act (PDPA), which came into full effect on 2 July 2014, comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data as well as the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

The trend of vast amounts of personal data being collected, used and even transferred to third-party organisations for a variety of reasons is expected to grow exponentially with increasingly sophisticated technology. With this trend comes growing concerns on the part of individuals about how their personal data is being used.

The PDPA presents a data protection regime to govern and address these concerns and to maintain individuals' trust in organisations that manage individuals' personal data.

By regulating the flow of personal data among organisations, the PDPA also aims to strengthen and entrench Singapore's competitiveness and position as a trusted, world-class hub for businesses.

Data Protection Obligations

Upon enactment in 2012, the PDPA had nine primary data protection obligations with which organisations are required to comply. As part of a review of the law (discussed in **1.7 Key Developments**), the Singapore Parliament passed amendments to the PDPA in 2020 adding two additional obligations.

Consent obligation

Private organisations can only collect, use or disclose personal data when an individual has given consent. If consent is given, organisations must inform individuals of the consequences of their withdrawal of consent. In the event that consent is withdrawn, organisations must cease all collection, use and disclosure of that individual's personal data.

Purpose limitation obligation

Organisations may collect, use or disclose personal data about an individual for the purposes for which they have given consent. Organisations must not use an individual's personal data for any reasons other than for the specific purpose set out between the parties.

Notification obligation

Organisations must state the purpose(s) for which they intend to collect, use or disclose individuals' personal data, and communicate this clearly to an individual before commencing data collection, use and disclosure.

Access and correction obligation

Individuals or subscribers of an organisation can request information on how their personal data has been used throughout the period for which they have given their consent. Organisations cannot decline such a request, and they are required to correct any error or omission in an individual's personal data upon such a request.

Accuracy obligation

Personal data collected by or on behalf of the organisation must be accurate and complete as far possible. Necessary parameters must be set in place to prevent any errors upon consent submission.

Protection obligation

When individuals have given organisations their trust, the latter should support and maintain that

trust. This is done by setting up the necessary security measures to safeguard the information in the possession or control of the organisation so as to prevent any form of unauthorised access to such information.

Retention limitation obligation
Once an individual's personal data is no longer necessary for any business or legal purposes, organisations must cease retention of the information or remove the means by which the personal data can be associated with the individual.

Transfer limitation obligation
In the event personal data is required to be transferred to another country for any reason, organisations should so do only according to the requirements prescribed under the regulations. Organisations should ensure that the standard of protection for any individual's personal data transferred is comparable to the protection under the PDPA in Singapore.

Accountability obligation
The accountability obligation states that organisations must make information about their data protection policies, practices and complaints process available, either on request or publicly.

Data breach notification obligation
Organisations are required to assess whether a data breach is notifiable, and to notify the affected individuals where required and/or the Personal Data Protection Commission where the data breach is assessed to be notifiable. A data breach is assessed to be notifiable where the scale of the data breach is of a significant scale; ie, where it involves the personal data of 500 or more individuals or the data breach causes significant harm to affected individuals.

Data portability obligation
Upon request from individuals, the organisation must transmit the individuals' data in its possession or under its control to another organisation in a commonly used machine-readable format.

The PDPA targets private organisations and emphasises good personal data management practice when collecting, using, disclosing and storing personal data about individuals. Compliance with the PDPA will increase an organisation's business efficiency and effectiveness, boost customer confidence, and enhance its public image.

1.2 Regulators

The Personal Data Protection Commission

The Infocomm Media Development Authority has designated the Personal Data Protection Commission (PDPC) in Singapore, to be responsible for the administration of the PDPA.

The PDPC was established on 2 January 2013 and serves as the primary authority in Singapore dealing with the administration and enforcement of the PDPA. It seeks to balance the need for protection of individuals' personal data and the needs of organisations to use personal data for proper and legitimate purposes.

The fundamental principle of the PDPA is accountability. Accountability is the undertaking and exhibition of responsibility for the personal data in the organisation's possession. Sections 11 and 12 of the PDPA provide for the accountability of organisations to comply with the PDPA. An accountable organisation is answerable to the relevant regulatory authorities and individuals who entrust the organisation with their personal data.

In the event of any data breaches, the PDPC will be involved to resolve the issues in question. The next level in the hierarchy, where a party is aggrieved by the decision or direction of the PDPC, is to make an appeal to the Chairman of the Data Protection Appeal Panel under Sec-

tion 34(1) of the PDPA. Should the party still be unsatisfied with the decision, they may appeal to the High Court and the Court of Appeal on points of law.

PDPC Powers

The PDPC has various powers to enforce the provisions contained in the PDPA. These powers may be summarised according to the powers relating to alternative dispute resolution, reviews and investigations (which will be discussed in more detail below). Whenever a complaint of a data protection breach is presented to the PDPC, the objectives of the PDPC, in order to resolve the issue, are:

- to facilitate the resolution of an individual's complaint relating to an organisation's alleged infringement of the relevant data protection provision(s);
- to ensure that organisations comply with their obligations under the PDPA; and
- in the event of a non-compliance, to take the appropriate corrective measure(s) and other necessary action to ensure compliance.

In some cases, the PDPC may conduct a review or an investigation of the matters in question and, depending on the outcome of the review or investigation, issue directions to the relevant organisation to take a certain course of action to rectify the issue(s).

1.3 Administration and Enforcement Process

Where a complaint is received, the PDPC may:

- resolve the complainant's complaint through dispute settlement resolutions such as mediation;
- direct an organisation to take a certain course of action in relation to an individual's request, upon the confirmation of the request in question; or
- determine whether an organisation is data protection-compliant and establish any contravention of the provisions in the PDPA.

Should the PDPC find that there is non-compliance, the PDPC can issue appropriate directions to ensure compliance and correction.

According to the Advisory Guidelines on Enforcement of the Data Protection Provisions, some of the measures that are undertaken by the PDPC include:

- encouraging self-resolution;
- referring a complaint to an organisation;
- facilitating resolution;
- referring a complaint to mediation; and
- directing parties to attempt to resolve the complaint.

In some cases, the PDPC may, pursuant to Section 27(2) of the PDPA, direct either party or both parties to resolve the complaint in a manner directed by the PDPC. Other than issuing directions for alternative dispute resolution, the PDPC may also choose to conduct a review pursuant to Section 28 of the PDPA. In particular, the PDPC may review, on the application of an individual, matters such as:

- an organisation's refusal to provide access to personal data requested by the applicant in a request under Section 21 of the PDPA, or a failure to provide such access within a reasonable time;
- where an organisation has requested a fee in relation to the applicant's access request or a correction request; or
- an organisation's refusal to correct personal data, as requested by the applicant, or a failure to make the correction within reasonable time.

In the event of a contravention of the PDPA, Section 50 of the PDPA confers powers of investigation upon the PDPC. Generally, the PDPC may commence an investigation on its own motion or via being presented with a complaint made against an organisation. It is worth reiterating that when the PDPC receives a complaint, or information of a similar nature, alleging a contravention of the PDPA provisions, the PDPC always considers if the underlying matter can be resolved using the methods stipulated above (ie, alternative dispute resolution) before initiating an investigation.

Remedies

An aggrieved party (usually the complainant) can seek remedies in the forms set out below.

Administrative remedies

The PDPC has the power to issue directions as it deems fit to ensure compliance. These directions may include, but are not limited to, ordering organisations to cease collecting, using or disclosing the personal data of another or to destroy personal data in contravention of the PDPA. The PDPC can also direct organisations to perform the necessary corrections to personal data or fine infringing organisations up to SGD1 million.

Civil remedies

Directions issued by the PDPC may be registered with, and enforced by, a District Court in Singapore. Aggrieved individuals are provided with the right to initiate civil proceedings against organisations for loss or damage suffered.

Criminal remedies

Prima facie, contravention of the PDPA will generally not amount to a criminal offence. However, the PDPA does provide criminal penalties in respect of "obstructive" actions, eg, refusing to correct personal data and/or falsifying, concealing or destroying information about the collection, use or disclosure of personal data.

1.4 Multilateral and Subnational Issues

Singapore supports open and transparent data flow across borders and data protection standards are in place to ensure that such exchanges occur in a responsive and protected environment.

On 20 February 2018, Singapore became the sixth Association of Southeast Asian Nations (ASEAN) economy to become part of the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems alongside other countries such as the USA, Mexico, Canada, Japan and Korea. Singapore is also the second APEC economy to participate in the Privacy Recognition for Processors System alongside the USA.

With the CBPR and PRP systems in place, organisations, after being certified by the PDPC, can exchange personal data with other certified organisations more efficiently, assuring consumers that cross-border transfer of their personal data is subject to high standards of data protection.

As Singapore is one of the European Union's largest trading partners in the ASEAN, many organisations inevitably fall under the jurisdiction of the EU's General Data Protection Regulation (GDPR). The GDPR protects the personal data of data subjects in the EU and is enforced by supervisory authorities who are independent public authorities established in EU member states.

Singapore organisations outside the EU must exercise compliance with the GDPR if those organisations either process the personal data

of individuals in the EU or monitor the behaviour of individuals in the EU.

1.5 Major NGOs and Self-Regulatory Organisations

All NGOs and self-regulatory organisations (SROs) in Singapore are subject to the same rules and regulations stipulated under the PDPA.

1.6 System Characteristics

The PDPA and the Public Sector

The PDPA has a limited scope of enforcement and the Act itself does not apply to all sectors. Notably, the PDPA does not apply to the public sector or government agencies. Public sector agencies are governed by the standards of data protection rules such as the Public Sector (Governance) Act 2018 (PSGA) and Government Instruction Manuals.

While a breach of any provision in the PDPA does not generally amount to a criminal offence, public officers who disregard the government's data security rules may, if found liable under the PSGA, be subject to penalties including fines of up to SGD5,000 or a jail term of up to two years, or both. Criminal liability of public sector bodies is generally no punished with fines because it was thought meaningless "to impose huge financial penalties on public sector agencies because the cost of such penalties would ultimately have to be borne by the same public purse" according to Minister for Communications and Information S Iswaran.

Exemptions to the PDPA

Furthermore, the PDPA does not apply to business contact information (ie, an individual's name, position or title, business contact number, business address, business email and any other similar corporate information) as this information is publicly available. Hence, organisations are not required to obtain consent for the collection, use or disclosure of (corporate) data.

Section 13 of the PDPA requires an individual to consent before their personal data can be revealed, collected, use or disclosed. Section 14 provides that if consent is obtained without the accompanying purpose being made known to the individual, then that consent is invalid. Similarly, if false, misleading or deceptive practices have been used, then there is no consent. However, the actual stringent operations under Section 13 are mitigated by the provision provided in Section 15 – Deemed Consent. This provision provides that consent can be deemed valid if an individual voluntarily surrenders and/or provides the personal data to an organisation for a purpose, and it is reasonable that the individual would voluntarily provide the data, without actually having to give consent.

Professor Hannah Yee Fen Lim, an Associate Professor at the National Technological University, has said that the provision is aimed at "achieving operational efficiency" where it does not require consent to be expressed or verbalised.

Another area concerns the right to access personal data. The PDPA provides individuals with access rights that ensure organisations must provide the relevant information about an individual's personal data and the purpose for the collection, use or disclosure of such data before, during and after such data is collected, use or disclosed. However, some organisations charge a (reasonable) administrative fee for such access.

1.7 Key Developments

National Registration Identification Card Numbers

One of the most notable developments in 2019 was the PDPC implementing stricter rules on the collection, use or disclosure of Singapore's National Registration Identification Card (NRIC) numbers. In a release published on 26 August

2019, the PDPA announced that, with effect from 1 September 2019, it will be illegal for organisations to physically hold onto an individual's NRIC and collect their full identification number, unless required to do so by law.

These rules aim to limit situations where organisations may collect and retain NRIC numbers without special regard to an individual's right to have their personal data protected. These rules stemmed from the recognition that NRIC numbers can be used to retrieve (personal) data relating to an individual. Moreover, an NRIC number is a permanent and irreplaceable identifier through which a large amount of an individual's personal information can be revealed. Negligent handling of NRIC particulars may also be used for illegal activities such as fraud and identity theft. Hence, the PDPC declared that "there is a need to reduce indiscriminate or unjustified collection and negligent handling of NRIC numbers".

Notwithstanding these new rules, the PDPC recognises that there are certain exceptional situations which require the collection, use or disclosure of NRIC numbers. These exceptions include specific situations where verification or records maintenance is legally required, such as when one seeks medical treatment, enrols in an education institution or joins an organisation for employment. There are, in addition, rare situations where personal data can be collected, used or disclosed without the individual's consent when an individual's life, health or safety is under imminent threat.

Amendments to the PDPA

The Singapore Parliament passed amendments to the Personal Data Protection Act 2012 on 2 November 2020, the first comprehensive review and change of the law since the PDPA's enactment in 2012.

Some of the key changes include:

- a shift away from the consent-based paradigm of the previous law by adding new exceptions to consent-based processing, including legitimate interests;
- the introduction of a right to data portability;
- new obligations to report data breaches to the PDPC;
- changes in the sanctions regime to increase penalties for individuals and organisations that breach the PDPA, including prison sentences; and
- enhancing the enforcement powers of the PDPC.

A company found guilty of a data breach can be fined up to 10% of its turnover. Currently the maximum fine is SGD1 million. The stiffer fine, however, will be imposed only on companies with an annual turnover exceeding SGD10 million. The amendment also allows organisations to collect, use or disclose personal data without the consent of individuals in circumstances where organisations have "legitimate interests" in doing so. Such situations include using the data from security cameras or other internet of things (IoT) devices to help in investigations or legal proceedings, or to recover/pay a debt.

Consumers must also be allowed to opt out of having their personal data used by companies such as e-commerce platforms to recommend specified items. Such recommendation engines typically analyse customers' browsing habits or previous purchases, for example, to automatically suggest items they would be more likely to buy.

COVID-19

A significant event in 2020, the worldwide COVID-19 pandemic has led to various responses, including techniques to track and monitor human movement. Organisations were permit-

ted to collect personal data of visitors to premises in Singapore. In the event of a COVID-19 case, relevant personal data could be collected, used and disclosed without consent during this period to carry out contact tracing and other response measures, as provided for under the "emergency" exception of the PDPA, where life, health or the safety of individuals are threatened.

Organisations may collect visitors' NRIC numbers, passport numbers and their equivalents for the purpose of accurately identifying individuals in the event of a COVID-19 case.

However, organisations that collect such personal data must still comply with the data protection provisions of the PDPA, such as making reasonable security arrangements to protect the personal data in their possession from unauthorised access or disclosure, and ensuring that the personal data is not used for other purposes without consent or authorisation under the law.

1.8 Significant Pending Changes, Hot Topics and Issues

A recent development involved the PDPC presenting the second edition of the Model Artificial Intelligence (AI) Governance Framework. On 23 January 2019, the PDPC released its first edition of the Model AI Governance Framework (Model Framework) at the 2019 World Economic Forum Annual Meeting (WEFAM) in Davos, Switzerland. The Model Framework provides detailed and readily-implementable guidance to private sector organisations to address key ethical and governance issues when deploying AI solutions. By explaining how AI systems work, building good data accountability practices, and creating open and transparent communication, the Model Framework aims to promote public understanding and trust in AI technology and its users.

On 21 January 2020, the PDPC released the second edition of the Model Framework at the 2020 WEFAM, also in Davos, which included additional considerations (such as robustness and reproducibility) and refined the original Model Framework for greater relevance and usability. For instance, the section on customer relationship management has been expanded to include considerations on interactions and communications with a broader network of stakeholders. The second edition of the Model Framework continues to take a sector and technology-agnostic approach that can complement sector-specific requirements and guidelines.

The release of an Implementation and Self-Assessment Guide for Organisations (ISAGO), intended as a companion guide to the Model Framework, aims to help organisations assess the alignment of their AI governance practices with the Model Framework. It also provides an extensive list of useful industry examples and practices to help organisations implement the Model Framework. ISAGO is the result of the collaboration with World Economic Forum's Centre for the Fourth Industrial Revolution to drive further AI and data innovation. ISAGO was developed in close consultation with industry, with contributions from over 60 organisations.

2. FUNDAMENTAL LAWS

2.1 Omnibus Laws and General Requirements

Data Protection Officers (DPOs)

The data protection provisions of the PDPA, specifically Section 11(3) of the PDPA, require an organisation to designate one or more individuals to be responsible for ensuring compliance with the PDPA. Section 11(4) provides that a person responsible for compliance with the PDPA may delegate the responsibility to another individual. Section 11(6) states that the designation of an

individual (or DPO) under Section 11(3) does not relieve the organisation of any of the obligations conferred on it by the PDPA. In other words, the legal responsibility for complying with data protection obligations remains with the organisation. The DPO(s) may be a person whose scope of work solely relates to data protection, or it can be a person in the organisation who takes on this role as an additional responsibility.

The PDPA does not prescribe where the DPO(s) should be based. They need not even be an employee of the organisation. Organisations may employ an outsourced DPO as a third party. Neither does the PDPA stipulate a deadline for an organisation to appoint a DPO. However, the PDPC encourages organisations to register their designated DPO at their earliest opportunity so the DPO can be kept abreast of the relevant data protection developments in Singapore.

The main responsibilities of an appointed DPO include:

- ensuring compliance with the PDPA when developing and implementing policies and processes for handling personal data;
- developing policies to handle personal data in electronic or non-electronic forms;
- conducting risk-assessment exercises to flag any potential data protection risks, and putting in place data protection policies to mitigate those risks;
- keeping employees informed of internal personal data protection processes and policies; and
- developing processes for handling queries or complaints from the public.

Privacy by Design or by Default

The concepts of "privacy by design" and "privacy by default" were introduced by the GDPR but their origins lie as far back as the 1970s. They make it compulsory for organisations to consider the ramifications of any personal data processing activities when developing a new or existing product or service.

Privacy by design holds that privacy should be an organisation's first consideration, especially at the initial design stage and throughout the development process of new products or services that involve processing personal data. Privacy by default refers to a service offering choices for to individual on how much personal data they wish to offer to the world and ensuring that the default setting in that situation is the most privacy-friendly one.

These concepts prescribe that privacy should always be an organisation's initial priority for every new product or service offered. However, they are rather difficult concepts to apply, especially when a design is completed. Embedding privacy is technologically challenging, expensive and sometimes even arduous. With that being said, transparency is key when it comes to earning the trust of individuals to share their personal data in the first place. Therefore, many organisations have already embedded the necessary factors in their development processes.

One should note however, that the concepts of privacy by design and privacy by default are purely theoretical. Presently, there is no precedent for a breach in PDPA obligations pertaining to privacy by design default theory. Moreover, it would be difficult to assess, should a case of this nature arise.

Privacy Impact Analyses

While the role of DPO is becoming an important one in every organisation, it is not uncommon to see DPOs being appointed with minimal knowledge of what the job truly entails. Although a DPO's responsibility is overseeing an organisation's entire data protection and privacy system, it would be helpful if they were equipped with

skillsets in multiple domains such as legal, IT, administration, cybersecurity and business analytics.

Such skills are necessary for a DPO to conduct a data protection impact assessment (DPIA). Once completed, a DPIA essentially places an organisation in a better position to handle personal data in compliance with the PDPA, complementary to their in-house data protection practices. To execute a DPIA, the DPO should first identify, assess and address the risks associated with personal data collection, use or disclosure. After assessing the risks, proper techniques can be implemented to safeguard the personal data of others.

The main ingredients in a DIPA involve the identification of personal data, the reason or purpose for collecting that data, identifying the risks associated with the intended action, and addressing those risks before executing a data collection activity.

In the event that risks involving large-scale processing of data or automated processing cannot be mitigated, proper and necessary steps such as consultations with the relevant authorities must be taken by the DPO.

Understanding risks also gives organisations room to experiment with new technologies and ways of protecting the personal data in their possession. Various regulatory sandbox methods are widely available, where organisations explore data sharing methods with less stringent rules within a controlled environment in order to better understand the implications of data collection. Singapore has always depended on the concept of "trusted data controllers" and recognition to give assurance to the public. For instance, organisations that have good data management platforms are often awarded trust certificates. These certificates strengthen the trust between the organisations and the public.

Anonymisation, De-identification and Pseudonymisation

In every organisation's operational data systems, sensitive information may be found for business or legal reasons. Organisations should not discount the possibility of data breaches and unauthorised access to their information systems either from unknown external sources or, with malicious intent, internally.

Such data security risks may be mitigated through the use of anonymisation, de-identification and pseudonymisation methods. This article briefly discusses each of these methods.

Anonymisation

Anonymisation is a process whereby personal data is transformed so that the information is not easily identifiable and linked to individuals. The anonymisation process is a set of risk management controls for mitigating personal data leakage and, in circumstances where individuals need not be identified for the purposes in question, it is usually a good practice to collect, use or disclose personal information in an anonymised form.

There are many ways to anonymise personal data. Examples include, inter alia, aggregation, replacement, data suppression, data shuffling and masking. However, the PDPC does not specifically recommend or endorse the use of the techniques mentioned above, so organisations should make their own independent assessment of the context in question before deciding to adopt one of the techniques. Not all information has to be, or can be, effectively anonymised.

Another important point to note is that, while they are in the process of anonymising their data, organisations should consider conducting

a DIPA to ascertain any potential negative (or positive) impacts on individuals before anonymisation, after anonymisation and when they can be re-identified.

De-identification

Another method, known as de-identification and similar to anonymisation, involves a range of techniques such as randomisation of subsampling or swapping. Simply put, it is removing personal data from a record. The removal process, however, is controlled. In this technique, organisations need only remove information that directly identifies an individual and in circumstances where there is a reasonable expectation that information about an individual could be used to identify that individual.

Pseudonymisation

Finally, pseudonymisation involves replacing personal identifiers with other random references such as a reference number or a coded tag that has been randomly generated. It is the processing of data in a manner in which the data can no longer be attributed to a category without the provision of other related materials.

Pseudonymous data is suitable for a great range of analytical activities, research projects and for statistical purposes. Because not all personal data is exposed, it decreases the risk of abuse of the exposed data in the case of a data breach. Pseudonymising the data may provide a "suitable measure" to safeguard data subjects' rights, freedoms and legitimate interests.

Injury or Harm

There is currently no requirement under the PDPA to prove "harm" or "injury" to establish wrongdoing. It is important to note that the data protection provisions under the PDPA do not affect any obligations or rights under other laws, neither do the PDPA provisions override or prevail over the other statutory provisions in Singapore. The PDPA shall not become a piece of legislation that prevents an individual from disclosing information if they are legally required (by other laws) to do so.

Leaking or disclosing personal data results in hefty fines under the PDPA. Certainly, trust between members of the public and organisations will fall and corporate confidence will be lost. Consequently, the organisation would need time to "repair" the damage and recover the public's confidence.

The PDPC is set up to oversee these issues and try to mitigate the loss, in an expeditious manner, including reviewing complaints and carrying out investigations which in turn, assure individuals that actions are being taken pertaining to their complaints.

In 2018 and 2019, the PDPC published over 40 enforcement decisions involving personal data breaches and issued the appropriate fines. These cases included a case involving Grab-Car Pte Ltd, where the PDPC imposed a fine of SGD16,000 to the organisation for failing to put in place reasonable data protection protocols to protect the personal data of its customers from unauthorised disclosure. The PDPC also imposed a fine of SGD20,000 on a Singapore company, WTS Automotive Services Pte Ltd, for allowing the unauthorised disclosure of some of its customers' personal data.

2.2 Sectoral and Special Issues

The PDPA provisions provide a baseline standard of personal data protection policy across the board. This is achieved by complementing sector-specific regulatory policies, where organisations are required to comply with the PDPA as well as the common law and other relevant laws that are applied to the specific industry to which they belong, when collecting, using and disclosing personal data.

This is unlike other jurisdictions, such as the USA or the EU, where the sectoral issues concept originated and where they are extremely particular and sensitive to personal data regarding health records and numbers, personal rights, sexual orientation/preferences and trade union membership. In Singapore, the PDPA does not specify the issues or the records and numbers of personal data. However, Singapore has enacted laws tailored to certain categories of data such as financial, health, communications and employment.

For example, for financial data, there are several governmental bodies, such as the Ministry of Finance, the Accounting and Corporate Regulatory Authority, the Monetary Authority of Singapore, etc. For health, there is the Ministry of Health, and the different Acts that regulate personal data. There is also the Ministry of Manpower which oversees employment matters.

Lastly, for communications data, Singapore has enacted the Protection from Online Falsehoods and Manipulation Act (POFMA), which Act seeks to prevent electronic communication of falsehoods. Although it does not specifically regulate personal data per se, it complements the PDPA as its objectives sometimes require the content creator to remove certain sensitive or personal information published in public domains.

It is worth reiterating that the PDPA does not apply to governmental bodies as they are regulated by legislation that is stricter than the PDPA. Therefore, the various ministries have a wider scope of flexibility to oversee matters pertaining not only to personal data but an array of other issues.

Securing Personal Data

Pursuant to the Protection obligation (as discussed in **1.1 Laws**), under Section 24 of the PDPA, organisations are required to make reasonable security arrangements to protect personal data and to prevent unauthorised access, collection, use, disclosure, leaks, etc. The PDPC has provided a guide titled "Guide to Securing Personal Data in Electronic Medium". The guide provides information on topics related to security and protection of personal data in electronic form and practices that organisations can adopt to enhance their data protection policies.

The PDPC states that the guide is not a one-size-fits-all solution on which organisations should have full reliance. It merely acts as an accessory to support or strengthen the organisations' existing data protection protocols because some organisations may adopt a different kind of electronic storage system to safeguard personal data. Security and data breaches involving personal data over the internet vary and can include, but are not limited to, hacking, gaining unauthorised access, phishing emails, malware, loss of hardware, compromised networks, unintended disclosure of personal data to a third party, etc.

The PDPC recommends that organisations manage their data protection policies using four governing principles: (i) accountability; (ii) standard, policies and procedures; (iii) risk management; and (iv) classification and tracking. The most relevant principle to this topic is classification and tracking. The PDPC recommends that organisations conduct periodic checks for personal data stored in electronic systems, conduct physical inventory and hardware checks regularly, update their anti-virus systems and ensure that their electronic means of storing personal data are up to date. Although this does not address personal data breaches directly, it is the organisation's first line of defence against any unpredicted cyber-attacks.

2.3 Online Marketing

With respect to unsolicited telemarketing communication, the PDPC has set up the Do Not Call Registry (the Registry). Members of the public are able to register their number with the Registry to avoid receiving unsolicited calls or texts and fax messages. Even though there is no cap on the number of registrants, not all private organisations are affected by this regulatory body. Organisations such as banks and telecommunication companies who have ongoing relationships with their customers are exempt from checking with the Registry in an intended marketing communication, as long as the customers are given the option to unsubscribe from the marketing content.

The Registry takes a serious view of unsolicited phone calls or text messages to those who have registered their numbers with the Registry to avoid just such unwanted marketing communications. It prevents telemarketers from calling and disturbing those already registered with the Registry. If they do, they risk a fine of SGD10,000 for each offence or face a maximum fine of SGD1 million.

Despite the good intentions of the Registry, it has been reported that an estimated 600 organisations continue to text or call numbers listed without permission and at least 3,700 complaints have been filed with the Registry. It can be argued that, given the advanced state of contemporary communications technology, the Registry perhaps needs to work with other platforms, such as WhatsApp, Telegram or Facebook to minimise unsolicited marketing and advertisements.

2.4 Workplace Privacy

Workplace privacy, including the rights of employers to monitor workplace communications are not specifically addressed by the PDPA. In Singapore, the Ministry of Manpower governs the collection and use of data relating to employments matters. Whistle-blower hotlines are not commonly implemented in Singapore, save for a number of hotlines where members of the public can direct any complaints.

2.5 Enforcement and Litigation

The PDPC is conferred with enforcement powers under the PDPA to rectify data protection violations.

When the PDPC receives a complaint from an individual, it will first review/address the individual's concerns by facilitating communication between the individual and the organisation. The PDPC may exercise its enforcement power under Section 29 to direct parties to take a certain course of action after the PDPC has reviewed the dispute in question. If both parties are unable to procure a resolution, the PDPC may refer the matter to mediation, though only if both parties agree to this. The PDPC may also direct parties to resolve the issue through alternative dispute resolution until an amicable solution is achieved.

The general offences and penalties for violating a data protection provision are as follows:

Under Sections 51(3)(b) and (c) of the PDPA, it is an offence to:

- obstruct or impede the PDPC, its inspectors or other authorised officers in the exercise of their powers or performance of their duties under the PDPA; or
- knowingly or recklessly make a false statement to the PDPC, or knowingly mislead or attempt to mislead the PDPC, in the course of the performance of the duties or powers of the PDPC under the PDPA.

Enforcement Penalties

Any organisation which violates the above-mentioned provision is liable:

- in the case of an individual, to a fine not exceeding SGD10,000 or to imprisonment for a term not exceeding 12 months, or to both; and
- in any other case, to a fine not exceeding SGD100,000.

When the PDPC decides to issue financial penalties, it refers to a non-exhaustive list of aggravating and mitigating factors to determine the weight of the intended penalty. Aggravating factors may include, but are not limited to, failure to actively resolve a dispute with an individual in an effective and prompt manner, intentional or repeated violations of the PDPA provisions, or failure to comply with the PDPC's directions. Some examples of mitigating factors are early settlement of a dispute with the relevant individual, the organisation taking reasonable steps to reduce the harm resulting from the breach/violation, or voluntary disclosure to the PDPC of a breach at the earliest opportunity.

Private Litigation

Apart from complaints received by the PDPC, there are no reported cases of private litigation cases taken out for privacy violations or personal data breaches.

Class actions are generally allowed in Singapore, only if approved, and after obtaining the necessary licences from the relevant authorities. However, if a class of individuals wish to pursue an action against, for example, SingHealth because of a data leak, it is unlikely to succeed in the Singapore courts.

3. LAW ENFORCEMENT AND NATIONAL SECURITY ACCESS AND SURVEILLANCE

3.1 Laws and Standards for Access to Data for Serious Crimes

The handling of serious crimes by law enforcement agencies is excluded from PDPA coverage and its corresponding provisions with regards to data subjects' rights to data privacy.

3.2 Laws and Standards for Access to Data for National Security Purposes

There is legislation that governs confidential information, anti-terrorism issues and other national security matters. These statutes include, but are not limited to, the Official Secrets Act, the 2012 Internal Security Act, the Serious Crimes and Counter-Terrorism (Miscellaneous Amendments) Act 2018, and the Terrorism (Suppression of Financing) Act.

There is no legislation in Singapore that requires additional authority for the government to access data for national security purposes.

3.3 Invoking Foreign Government Obligations

The provisions of the PDPA do not provide for the invocation of a foreign government's request as a basis on which to collect or transfer data.

3.4 Key Privacy Issues, Conflicts and Public Debates

Since the PDPA came into full force, there have been a number of reports clarifying the rationale of government agencies being immune to it and the reasons why it does not apply equally to government organisations and private organisations. Privacy advocates have raised concerns about the lack of transparency of the public sector's data security standards. One of the key recommendations suggested to improve transpar-

ency is to publish the government's policies and standards relating to personal data protection and to provide an update on an annual basis.

As the government maintains that the public sector is governed by a different set of more stringent rules, privacy advocates are asserting that publishing the policies will allow the public to see for themselves if this is so, at the same time they can be assured that their personal information is best protected. Another advocate asserts that publishing the standards which the government has adopted would allow private organisations to better understand the ideal standards that have to be met.

As much as these advocates hope for greater public awareness of data protection standards, presently, there is no indication that these ideal principles will be shared publicly. Meanwhile, private organisations are free to consult the PDPC for any data protection queries that they may have in the future. Similarly, the PDPC is constantly publishing reports on the latest updates on data protection, which are equally beneficial to private organisations.

4. INTERNATIONAL CONSIDERATIONS

4.1 Restrictions on International Data Issues

Under the data protection guidelines, both Section 26 of the PDPA and the Transfer limitation obligation (see **1.1 Laws**) limit the ability of an organisation to transfer personal data outside of Singapore. Section 26(1) of the PDPA expressly states that an organisation must not transfer personal data to a country or territory outside Singapore, except in accordance with the requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so-transferred that is comparable to the protection under the PDPA.

4.2 Mechanisms or Derogations that Apply to International Data Transfers

There are no mechanisms applicable in Singapore to international data transfers. Safety data mechanisms should be developed between the private organisations and the intended recipients. The PDPA is silent as to whether such mechanisms should be adopted as part of its obligations.

4.3 Government Notifications and Approvals

Generally, there is no requirement for organisations to seek government approval to transfer data internationally as the local government does not rely on the PDPA provision, per se. Any data that is intended for a recipient based outside of Singapore must comply with the procedures set out under the PDPA.

For export and import purposes, there are a different set of laws (such as contract law or the Regulation of Imports and Exports Act) that regulate international transfers. However, personal data would not fall under this category.

4.4 Data Localisation Requirements

India recently proposed, in the Personal Data Protection Bill 2019, (akin to the GDPR) that companies in India will be required to gather the consent of Indian citizens before their data can be collected and processed. At the same time, the new rules also state that companies would have to hand over the "non-personal" data of their users to the government, and New Delhi would also hold the power to collect any of the data of its citizens without their consent to serve the larger public interest.

In contrast, there are no such data localisation requirements under Singapore's PDPA. Many

organisations are also less supportive of data localisation. Ravi Menon, Managing Director of the Monetary Authority of Singapore, at the Singapore FinTech Festival of 2018, stated that "We need more data connectivity, and less data localisation. This is a serious risk".

In the current digital era, big companies operate across digital borders by setting up cloud networks of data centres. This means that an individual's data can reside anywhere and anytime. "Data localisation measures are on the rise around the world. If data cannot cross borders, the digital economy cannot cross borders and we will be poorer for it", said Menon.

4.5 Sharing Technical Details

The PDPA does not provide specifications or standards that enable or require the sharing of technical details with the government of Singapore in regard to data protection issues.

4.6 Limitations and Considerations

Consular support and assistance are often provided to assist other jurisdictions in areas such as law enforcement, disaster response, etc. However, the PDPA is silent as to how local government might respond to a foreign government's data request. Neither does Singapore report such foreign data requests publicly, partly because some of these requests (if they exist at all) are confidential by nature.

4.7 "Blocking" Statutes

Singapore does not have specific "blocking" statutes but does have general statutory provisions that prevent the disclosure of matters relating to the national interest.

5. EMERGING DIGITAL AND TECHNOLOGY ISSUES

5.1 Addressing Current Issues in Law

Amid the proliferation of cybersecurity threats and digital-based data breach incidents in the past two years, Singapore has continued to develop its data protection, cybercrime, and cybersecurity regimes. As detailed in Singapore's Cyber Landscape 2019 report, Singapore focuses on four pillars in its strategy to protect the country from cyberthreats and reinforce Singapore's standing as a leading information systems hub. The key legal components in this strategy include the Personal Data Protection Act 2012 (PDPA), the Computer Misuse Act (CMA) to combat cybercrime and other cyberthreats, and the Cybersecurity Act 2018 (Cybersecurity Act), which focuses on protecting Singapore's Critical Information Infrastructure (CII) in 11 critical sectors and establishing a comprehensive national cybersecurity framework.

Regular collaborations by the PDPC with the Cyber Security Agency of Singapore (CSA) and the Singapore Police Force (SPF) has resulted in various public education efforts; an example being a November 2021 handbook providing an overview of the Cybersecurity Act, CMA and PDPA; information on how these three different pieces of legislation work in tandem; and illustrative examples of data breaches. It also provides online resources to assist organisations in securing their IT systems and to help individuals protect their data.

Big Data Analytics

Regulation of big data analysis relates to the consent obligation under the key principles of data protection, in particular, to the need to obtain consent before an organisation conducts analysis and research activities. It is true that any organisation intending to carry out research activities which require the collection, use or dis-

closure of personal data needs to comply with the PDPA. The participants should be informed of the purposes for which their personal data is collected, used and disclosed by the organisation.

Currently, organisations may use personal data without consent if they do so for research purposes. This is reflected under paragraph 1(i) of the Third Schedule of the PDPA. More specifically, the paragraph states that an organisation may use the personal data of an individual, without the consent of that individual, if the personal data is used (solely) for research purposes. However, the provision shall not apply unless:

- the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;
- it is impracticable for the organisation to seek the consent of the individual for the use;
- the personal data will not be used to contact persons to ask for participation in the research; and
- linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

Automated Decision-Making

The above also relates to obtaining consent at the outset, before automated algorithmic decisions can come into play. For AI to benefit organisations and businesses, additional principles ought to be incorporated into the AI governance framework.

Decisions made by or with the assistance of AI should be explainable, transparent and fair to sustain trust and confidence in those automated decisions. Also, decisions made by AI should be human-centric. The concept of human-centric refers to an approach that puts the individual at the forefront of plans for AI deployment. Organisations that are perceived to have caused harm to consumers as a result of their AI deployment do not inspire consumer trust and confidence. The key ingredient in having automated decision-making feature in a process is beneficence, or the "no harm" principle. The no-harm principle refers to decisions that should not cause foreseeable harm to any individual and decisions that should always strive to confer benefits or assistance instead of liability.

The PDPA in Singapore is silent on the creation of automated decision-making but expects organisations to actively initiate the appropriate framework for automated decision-making features, while remaining fully compliant with the PDPA. This is the case for AI (including machine learning), autonomous decision-making (including autonomous vehicles) and data profiling.

Internet of Things (IoT)

The IoT, thought by some to be the next big technological revolution, is the process in which devices like mobile phones and security cameras are connected to the web. As Singapore aspires to be a "Smart Nation", it is already evident that the country's cloud infrastructure, broadband service, the ease of conducting business and controlling the flow of traffic are facilitating the growth and advancement of the IoT.

The context of the IoT in Singapore is moving away from the idea of data protection and towards data collection to improve the country's efficacy and efficiency. Take for example, controlling the flow of traffic on a daily basis. Currently, the traffic is managed by electronic road pricing (ERP) systems, an electronic toll collection scheme and usage-based mechanism. The ERP system, apart from collecting tolls, also collects data: the number of cars that pass certain expressways daily. The relevant government agencies then use this anonymous data

to enhance and improve their traffic management procedures. Recently, the Land Transport Authority of Singapore (LTA) announced a new implementation of ERP in which features will be added to improve the driving experience and better manage daily road traffic conditions.

The PDPA is silent as to the governance structure applicable to the IoT, rather, it is left to the respective organisations to decide where they intend to improve on and enhance their existing data protection protocols.

Facial Recognition

Facial recognition has become common in daily life, most notably through Apple's face ID, as well as security counters at immigration checkpoints. Essentially, facial recognition is another form of verifying one's identity. Singapore is taking a more progressive approach to technological advances in this area, which prompts the question: what are the implications of allowing such pervasive surveillance for the sake of convenience? Surely, facial recognition systems open new possibilities for potential abuses of power, profiling and non-consensual data collection.

Disinformation and Other Online Harms

As of 1 January 2020, Singapore has enacted a new law around "doxxing" under the Protection from Harassment Act (POHA). Doxxing occurs when an individual or entity publishes the personal information of another individual or a group of individuals in order to harass, threaten or facilitate violence against them. To a certain extent, it correlates with the PDPA in prohibiting the publication or misuse of personal information about an individual. However, the new laws are much narrower as, under the amended Section 3 of the POHA, a person may be guilty of an offence if they publish personal information about another person with the intention of causing distress, harassment or alarm, even though the personal information has not been shared with others.

5.2 "Digital Governance" or Fair Data Practice Review Boards

The word "reasonable" is mentioned approximately 48 times in the PDPA. This word implies that the PDPC requires organisations to put in place necessary and suitable data protection protections. Although there is no strict governing framework imposed on organisations to execute a certain course of action within a stipulated time, organisations are expected to take initiative(s) to handle their own protocols from the outset. The PDPC only gets involved when a complaint has been lodged.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation.

Currently, all enforcement is performed by the PDPC. There is no real litigation per se – ie, an individual bringing an action against the state in relation to privacy laws.

The PDPA is an act that protects an individual's personal data. It is not an act that allows individuals to bring an action against another individual or even against the state. As far as litigation is concerned, there are no reported cases where an applicant has successfully litigated on a privacy law matter and obtained redress or compensation.

5.4 Due Diligence

With regard to corporate transactions, organisations are expected to perform their due diligence to ensure that every transaction, regardless of whether it contains data collection elements, is fully compliant with the relevant laws and/or procedures. Performing due diligence means to embark on a process of verification, investigation, audit and confirmation of all relevant facts and details. In essence, it is about doing ample

and adequate research before entering into an agreement or completing a transaction.

Under the law, it is known as performing a legal health check. Due diligence is a risk assessment for organisations to adopt in order to address potential issues. The ultimate goal is to fully understand the legal situation of a company and the issues that company may face post-transaction.

5.5 Public Disclosure

The PDPC maintains a position of providing transparent and full public disclosure of its enforcement decisions. These decisions provide salient insights from which organisations are strongly encouraged to take guidance, and to implement measures to prevent similar occurrences. The publication of cases on the PDPC's website aims to promote accountability among organisations and to safeguard consumer interests and trust.

5.6 Other Significant Issues

There are no other significant data protection and privacy issues in Singapore not already covered in this chapter.

Aequitas Law LLP is a full-service law practice with ten fee earners. The firm has an established track record of advising and consulting with organisations and individuals on the establishment and administration of all matters connected with the collection, use and disclosure of personal data by organisations. The firm's deep expertise in data protection and privacy encompasses both technical expertise in the fields of information privacy and privacy programme management as well as legal expertise in contentious and non-contentious matters. Recent work and representation in this area includes consulting and representing a town council, commercial corporations, and residential and commercial developments.

AUTHORS

Tat Lim is a founding partner of Aequitas Law LLP. He has more than 30 years of experience as counsel and in dispute resolution across a wide spectrum of matters. Apart from his legal practice, Tat is also an accredited mediator and arbitrator with many distinguished institutions. He is widely recognised as a global leader in mediation, and his legal practice has been internationally ranked. He is a contributor to various publications on his areas of practice, including civil procedure and mediation in Singapore. He also serves as a member of the editorial boards of international publications on dispute resolution.

Chiew Khoon Heng is a data protection manager for Aequitas Law LLP and an independent data protection consultant certified by the International Association of Privacy Professionals, a non-profit, non-advocacy membership association founded in 2000 providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, and standardise the designations for privacy professionals. He is also a practising data protection officer providing consultancy and services for implementing and managing data protection infrastructure for diverse organisations.

Aequitas Law LLP

28 Maxwell Road
#04-05 Maxwell Chambers Suites
Singapore 069120

Tel: +65 6535 0331
Fax: +65 6535 0131
Email: tat@aqt.sg
Web: www.aequitasllp.com

Trends and Developments

Contributed by:
Tat Lim and Chiew Khoon Heng
Aequitas Law LLP see p.27

The Enhanced Personal Data Protection Act and Considerations in the New Digital Economy

Singapore's Personal Data Protection Act 2012 (PDPA) establishes a data protection law that articulates protection via "obligations", that is, acts or courses of action which an "organisation" (as defined in the PDPA) is legally bound to perform, including the discharge of duties or commitments regarding which compliance to the Act is required. Chief among the obligations is the principle of consent; individuals must consent or be deemed to have consented before collection, use or disclosure of personal data is permitted. In addition, consent is considered valid only when individuals are notified and informed on the purpose for the personal data collection.

The PDPA can be considered a "consent-first" law, that is, consent to collection, use or disclosure of personal data is always required, unless there is an exception to the need for consent. In contrast, the European Union's General Data Protection Regulation (GDPR) treats consent as the correct lawful basis only if no alternative is available. The PDPA provisions allow individuals to withdraw consent and to be informed of the likely consequences of such withdrawal.

On 2 November 2020, the Personal Data Protection (Amendment) Bill (Bill) was passed in the Singapore Parliament, following its introduction in October 2020. The Bill sought to amend the PDPA by:

- strengthening the accountability of organisations in respect of the handling and processing of personal data;
- enhancing the legal framework for the collection, use and disclosure of personal data;
- providing individuals with greater autonomy over their personal data; and
- enhancing the enforcement powers of the Personal Data Protection Commission (PDPC).

In force since 1 February 2021, the enhanced PDPA introduced an expanded consent framework, with two new forms of consent: deemed consent by contractual necessity and deemed consent by notification. New exceptions to the consent regime can be applied, including using, collecting or disclosing data for legitimate interests, business improvement and commercial research and development; and if the legitimate interests of the organisation and the benefit to the public exceed any adverse effect on the individual.

The PDPA and the advent of the digital economy

The digital economy refers to the production and consumption of goods and services together with the supply of money based on information and communication technology (ICT), and is increasingly perceived as conducting business through markets using the internet and the World Wide Web. Also referred to as the "Internet economy", "new economy", or "web economy", it encompasses everyday online interconnectedness among people, businesses, devices, data and processes using the Internet, mobile devices and the internet of things. Given that one of the PDPA's goals is to address the increasing use of personal data in the face of rapid technological advancements and deeper complexities associated with the digital economy, it may be said that

the PDPA does not attempt to accentuate the role of consent in Singapore's data protection model, instead adopting a balancing approach incorporating necessity, reasonableness and fairness not secured by the consent obligation.

Increasing the emphasis on the PDPA's protection obligation and accountability obligation may prove a better strategy to encourage more effort and resources being put in place to build trust and safeguards within organisations. The protection obligation is an organisation's responsibility to make reasonable security arrangements to protect individuals' personal data in its possession so as to prevent unauthorised access, collection, use, disclosure or similar risks. The accountability obligation is an organisation's responsibility to make information about data protection policies, practices and complaints process available upon request to the public and to designate a data protection officer (DPO).

In 2017, the Personal Data Protection Commission (PDPC) proposed to reduce the significance of consent partly because of its inconvenience to the practice of personal data analytics, reducing its role to "where seeking consent is practical" by developing "parallel bases for collecting, using and disclosing personal data". Instead "greater responsibility would be placed on organisations to demonstrate accountability in ensuring the protection of personal data and safeguarding the interests of individuals".

A measure of how this responsibility has been found lacking may be observed in PDPC enforcement decisions relating to organisations found to have contravened the data protection provisions under the PDPA. A local news article on 2 November 2021 reported that 68% of the total number of data breach incidents recorded from April 2016 to October 2021 involved a breach of the concerned entities' protection obligation. Learnings include businesses relying on servers insufficiently protected with weak passwords, former staff's access still being available and customers' ordering or membership data being exposed due to insecure protocols. The move to transacting online via the Internet has enabled social engineering and phishing attacks by malicious parties and introduced new cybersecurity risks such as ransomware. The mass shift to working from home due to the COVID-19 pandemic created challenges in information technology infrastructure, especially in the area of access security, resulting in not insignificant stress for small and large organisations alike. While the protection obligation's percentage share of the total number of data breach incidents certainly contributes to an interesting headline, details of the incidents themselves are perhaps more indicative of the downsides that the digital economy has brought.

Weakening of the effectiveness of consent

The manifestation of the digital economy is best illustrated through the establishment of e-commerce portals and marketplaces (for example, Amazon.com Inc). The modern Internet marketplace commonly performs an aggregation role of matching supply (sellers) and demand (buyers). It is in the interest of this marketplace to accumulate maximal numbers of each party for revenue maximisation at minimal costs. In 2017, The Economist published a story titled "The World's Most Valuable Resource Is No Longer Oil, but Data". It aptly summarises the thinking that raw data (like crude oil) is not valuable in itself, but rather, when gathered completely and accurately, connected to other relevant data, and processed in a timely manner, new value (like petroleum and jet fuel) is created or realised. It also underscores that for such marketplaces to thrive, data collection and, inevitably, personal data collection of buyers (who normally outnumber sellers) is the actual profitable business. Significant revenues may be generated through large data sets that may be analysed computationally to reveal pat-

terns, trends, and associations, especially relating to human behaviour and interactions (otherwise known as "big data").

With the need for personal data collection, so follows the "privacy policy" or "notice". Agreeing to the terms as stated in such documents constitutes consent as defined by most privacy or data protection laws. However, the presupposition of all consent lies in the assumption that the terms are understood and the consent decision is informed. This state can only occur if the privacy policy or notice is actually read and understood.

Numerous published surveys on the content, language and length of modern privacy notices of larger organisations reveal that they have become onerous to read and understand, and that the precautionary legalese, vague and elastic form of language may be (if viewed cynically) a deliberate legal risk management strategy. A New York Times article (2 February 2019) "How Silicon Valley Puts the 'Con' in Consent" reports: "The average person would have to spend 76 working days reading all of the digital privacy policies they agree to in the span of a year. Reading Amazon's terms and conditions alone out loud takes approximately nine hours." Whether valid or not, such strategies may be tested in the courts of law, most likely only when challenged. All of the above results in "consent fatigue" and "consent erosion", whereby consent evolves into a much less effective safeguard for personal data protection.

The oft-quoted scope of consent, that pertaining to the collection, use and disclosure of personal data, is normally presented in this three-step "bite-sized" version for conciseness. Upon further elaboration, the complete personal data "life cycle" is then presented with the addition of the storage, retention and disposal phases. Critically, however, the actual control an individual possesses over providing (or denying) meaningful consent beyond the collection phase may be doubtful, or often reduced to deciphering "word play" within the privacy notice.

For most Internet portals, the widely accepted practice of creating a "user account" before commencement of usage is the only opportunity for an individual to provide consent, without which "account verification and creation" cannot proceed and the individual is reduced to a read-only "browsing" person, defeating the objective of the consumer (to, well, consume) in the first place. While the PDPA does provide objections against this scenario of "no consent – no product/service", as commonly articulated, it may not be properly enforceable when organisations use bundled consents against a broad range of operations and purposes, justified with difficulties related to interconnected product classes, operational process complexities or an inadequately defined network of intermediaries.

Lastly, the use of data intermediaries, a notable characteristic of a modern digital economy, commonly poses significant challenges for larger organisations when determining actual data flows, lines of control and the extent of data sharing. While the PDPA imposes only the protection and retention limitation obligations directly on data intermediaries, a study of sample PDPC enforcement cases involving data intermediaries reveals that many organisations become complacent, and neglect governance and risk management aspects, with poor oversight and policies contributing to PDPA compliance issues. While such organisations, as data controllers, may logically be expected to articulate the nature of the consent given by individuals to include its data intermediaries, in practice individuals may need to invest time and effort to investigate and discover their personal data's "exposure" to each data intermediary before arriving at a consent decision. For individuals,

expending such effort goes against one of the basic premises of the digital economy: that of increased speed and efficiency for all.

All of the above factors contribute to the weakening of consent effectiveness in the classical data protection toolbox, perhaps relegating it to an easily understandable "concept" but one given lower priority compared to the rigours of a modern digital economy demanding speed, lowest cost and other productivity or efficiency metrics.

Consent withdrawal in the digital economy: concept meets reality

The digital economy heralded a new paradigm applying especially to software and services; a "free" use model on a time-limited or perpetual basis. News, literature, computer games, interesting but untested software concepts, useful software utilities, even physical deliveries and product samples, for example, could now be obtained on a no-cost basis.

An oft-quoted saying, "When a product is free, the user is the product", attempts to explain the true business model of this new paradigm. In April 2018, a public statement by Facebook's chief executive Mark Zuckerberg, who plainly said Facebook sells advertisements (for profit), concisely explained this new paradigm. Facebook's business model is based on offering its tools and services mostly for free to billions of users and then making money by allowing businesses to show advertisements to Facebook's users. Advertisers pay a price to Facebook that is determined in an auction, based on supply and demand.

In the Facebook-Cambridge Analytica data breach incident of March 2018, the acquisition of up to 87 million Facebook users' personal data by Cambridge Analytica (with no explicit permission given to Cambridge Analytica) highlighted the scale on which Facebook had access to its users' personal data, the ease with which such data could be shared without its users' knowledge and, most importantly, the fact that the data sharing had been going on for an extended period despite Facebook's public pronouncements and assurances on data privacy.

In effect, the "free" model has created a subtle change in the psyche of "netizens". When an individual's mental cost-benefit analysis initially stands at zero cost and all benefits, the subsequent inclusion of the "cost" of possibly sharing personal data for perhaps unknown purposes and in the absence of notifications is also discounted to zero. In fact, the utility of sharing more personal data may be increased, as in the case of Facebook usage, if more "friends" can be found.

This phenomenon is not limited to social media platforms like Facebook. Users of online mapping tools, for example Google Maps, may value the utility and convenience, and even marvel at the ingenuity of the software with nary a concern that where Google is concerned, nothing is more valuable than knowing users' locations. In a lawsuit brought by the state of Arizona in the USA, Google executives had worked to develop technological workarounds to keep tracking users even after they had opted out. Rather than abide by its users' preferences, Google allegedly tried to make location-tracking settings more difficult to find and pressured smartphone manufacturers and wireless carriers to adopt similar measures. Even after users turned off location tracking on their devices or opted out, Google found ways to continue tracking them, according to a deposition from a company executive. In summary, a cynical analysis of this organisation's true objective in creating this software application may lead to the conclusion that it is not so much for assisting the lost; rather, it is

to collect even more data, which can be said to have belonged to individuals in the first instance.

Therein lies the dilemma: the perceived benefits of convenience, utility and, possibly, fun outweigh any personal data risk, yet to be realised in the absence of any bad news of data breaches or privacy violations. The granted consent, long forgotten or currently irrelevant, results in no requirement or motivation for consent withdrawal. As highlighted in the previous parts, withdrawal of consent may imply a full closure of the "user account", resulting in the total loss of benefits.

No doubt the digital economy at large does not solely comprise Facebook, Google or other platforms engaged in nefarious behaviour. However, the same "dulling" of individuals' perception of the value of and risk to their personal data largely exists, to the extent that any consent withdrawal, though understandable in theory, becomes impractical and possibly even unthinkable in reality. What would the current 2.7 billion monthly active Facebook users say to that? Would you stop using Google maps by withdrawing consent to the sharing of your location data with Google, which the mapping application states (logically) is necessary to mark your current geo-location?

The enhanced PDPA reflects the realities of consent

The original form of the PDPA, with its consent-centric characteristics, was increasingly out of place given the weakened effectiveness of consent in the rising digital economy for which data is a key enabler.

The traditional method for obtaining "all-or-nothing" consent, through the privacy notice mechanism, does not serve the interests of individuals well. The widespread use of data intermediaries in the digital economy complicates the consent relationship once thought to be simply between the individual and the organisation holding their personal data. Consent withdrawal in reality is far more complicated than what theory suggests. The marketplace's paradigm shift to "free" models in the digital economy has influenced individuals' behaviour in valuing other benefits above personal data protection. Consent withdrawal may have become a non-starting option.

The PDPA Amendment Bill presents a significant revision, aligning the PDPA with rising global standards and trends in data privacy laws. It represents Singapore's recognition of the rise of technology and technology-driven companies built on data utilisation for value creation in the digital economy. In particular, revisions to the consent framework including deemed consent exceptions provide organisations with more flexibility in legitimate personal data usage and individuals expending less attention on dealing with consent and consent withdrawal, falling in neatly with the digital economy's demands for higher productivity, speed of action and ultimately delivering the desired business improvements.

Aequitas Law LLP is a full-service law practice with ten fee earners. The firm has an established track record of advising and consulting with organisations and individuals on the establishment and administration of all matters connected with the collection, use and disclosure of personal data by organisations. The firm's deep expertise in data protection and privacy encompasses both technical expertise in the fields of information privacy and privacy programme management as well as legal expertise in contentious and non-contentious matters. Recent work and representation in this area includes consulting and representing a town council, commercial corporations, and residential and commercial developments.

AUTHORS

Tat Lim is a founding partner of Aequitas Law LLP. He has more than 30 years of experience as counsel and in dispute resolution across a wide spectrum of matters. Apart from his legal practice, Tat is also an accredited mediator and arbitrator with many distinguished institutions. He is widely recognised as a global leader in mediation, and his legal practice has been internationally ranked. He is a contributor to various publications on his areas of practice, including civil procedure and mediation in Singapore. He also serves as a member of the editorial boards of international publications on dispute resolution.

Chiew Khoon Heng is a data protection manager for Aequitas Law LLP and an independent data protection consultant certified by the International Association of Privacy Professionals, a non-profit, non-advocacy membership association founded in 2000 providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, and standardise the designations for privacy professionals. He is also a practising data protection officer providing consultancy and services for implementing and managing data protection infrastructure for diverse organisations.

Aequitas Law LLP

28 Maxwell Road
#04-05 Maxwell Chambers Suites
Singapore 069120

Tel: +65 6535 0331
Fax: +65 6535 0131
Email: tat@aqt.sg
Web: www.aequitasllp.com