IN-DEPTH

Privacy, Data Protection And Cybersecurity

SINGAPORE

LEXOLOGY

Privacy, Data Protection and Cybersecurity

EDITION 11

Contributing Editor

Alan Charles Raul

Sidley Austin LLP

In-Depth: Privacy, Data Protection and Cybersecurity (formerly The Privacy, Data Protection and Cybersecurity Law Review) provides an incisive global overview of the legal and regulatory regimes governing data privacy and security. With a focus on recent developments, it covers key areas such as data processors' obligations; data subject rights; data transfers and localisation; best practices for minimising cyber risk; public and private enforcement; and an outlook for future developments.

Generated: September 30, 2024

Singapore

Anna Toh
Amica Law LLC

Summary

INTRODUCTION
YEAR IN REVIEW
REGULATORY FRAMEWORK
INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION
COMPANY POLICIES AND PRACTICES
DISCOVERY AND DISCLOSURE
PUBLIC AND PRIVATE ENFORCEMENT
CONSIDERATIONS FOR FOREIGN ORGANISATIONS
CYBERSECURITY AND DATA BREACHES
SOFTWARE DEVELOPMENT AND VULNERABILITIES
DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY
OUTLOOK AND CONCLUSIONS
ENDNOTES

Introduction

Singapore adopts an omnibus data protection law: the Personal Data Protection Act 2012 (PDPA), to regulate the processing of personal data. On the surface, this approach is very similar to that of the European Union, however, their cultural and historical contexts are quite different: Singapore's data protection laws are concerned less with the concept of privacy and fundamental rights and more with positioning the jurisdiction as a trusted business hub. This is not to say that the law does not safeguard personal data from misuse, only that the rules and their application should be seen in this distinct light.

The PDPA applies to private organisations only. A separate framework governs data management in the public sector: the Public Sector (Governance) Act containing directions on data sharing, and the Government Instruction Manual on Infocomm Technology & Smart Systems Management. The rationale provided for this dichotomy is that more straightforward data sharing should be permitted between public agencies because the public expects them to provide services in an integrated manner.

Legal, cultural, and commercial attitudes toward data protection in Singapore have progressed since the PDPA was passed in 2013. Statistics published by the Personal Data Protection Commission (PDPC) show that enquiries and complaints were high in the first five years following the implementation of the PDPA but dropped in the following four years.[1] This reflects the public's growing awareness of their rights and businesses' journey toward compliance. The law has also moved from a primarily consent-based framework to one that acknowledges other legitimate bases for data processing.

On the cybersecurity front, Singapore has adopted the Cybersecurity Act 2018 (CSA) and the Computer Misuse Act 1993 (CMA). The CSA focuses on broader cybersecurity measures and applies to critical information infrastructure and cybersecurity service providers. On the other hand, the CMA focuses on individual criminal acts committed by malicious actors.

Additional guidance has also been issued for specific industries, with varying consequences for non-compliance. For example, financial institutions are subject to the Monetary Authority of Singapore's Technology Risk Management Guidelines, which aim to promote the adoption of robust practices for the management of technology risk. Healthcare providers are guided by the Cyber & Data Security Guidelines for Healthcare Providers and will soon be bound by legislation governing the sharing of health information.

Year in review

Two surges in the technology sphere drove changes in the data protection and cybersecurity landscape in Singapore in 2023: advanced artificial intelligence (AI) systems and cybercrime.

The swell in development and deployment of AI systems has shaken up businesses in Singapore. The government has identified AI as a 'strategic national priority', citing its potential to raise productivity, sustain competitiveness, and solve problems.[2] -

[] Acknowledging at the same time the need for strong AI governance, the regulatory authority has issued several guidance instruments, including the Model AI Governance Framework for Generative AI and the Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems. The extra-territorial impact of the European Union's AI Act will also be felt in Singapore. Many organisations are now grappling with technological, legal, and compliance requirements for adopting AI systems.

Cybercrime has been the other key force influencing data protection and cybersecurity in Singapore. Digital fraud attacks in the country are reportedly much higher than the average in the Asia-Pacific region, with bot attacks at more than five times the global average.[3] This is attributed to cybercriminals taking advantage of Singapore's status as an open and well-connected financial hub and its relative affluence.

The authorities have taken holistic measures to combat the rise in cybercrime. In 2024, lawmakers expanded the applicability of the CSA, acknowledging that it is not just critical infrastructure providers who may suffer attacks of national concern. The government's technology arm also works with the police and private corporations to roll out practical initiatives: in the past few years, it launched ScamShield (a suite of products the public can use to detect scams), PhishMonSG (a tool that detects phishing websites), and most recently, SATIS (a product that hunts and disrupts scam websites).

Several well-known companies have fallen prey to cybercriminals, resulting in substantial public interest data breaches. In late 2023, homegrown cashback portal ShopBack was fined US$54,600 over a data exfiltration incident affecting more than a million customers. In early 2024, Singapore-headquartered e-commerce platform Carousell was fined US$43,200 over two data breaches, the latter of which was a hacking incident involving more than two million customers' personal data. Both ShopBack and Carousell are widely used in Singapore, and these two episodes brought home to consumers the impact data breaches can have on them, the degree of data protection they can expect from companies, and the risks they face in an increasingly digitalised world.

Regulatory framework

Privacy and data protection legislation and standards

The Personal Data Protection Act 2012 (PDPA) and its subsidiary regulations govern the processing of personal data in Singapore. The regulatory authority, the Personal Data Protection Commission (PDPC), regularly publishes guidance documents to explain concepts in the PDPA and the practical application of the rules. Singapore does not recognise a general right to privacy.

The PDPA regulates the processing of personal data by organisations, but not processing by individuals acting in a personal or domestic capacity. An 'organisation' is a person, company, or other body of persons, located anywhere in the world, and embodies a concept similar to that of a data controller. Organisations which process personal data on behalf of another organisation are 'data intermediaries' and have limited obligations under the PDPA.

'Personal data' refers to data, whether true or not, about an individual who can be identified from that data on its own or together with other information to which the organisation has or is likely to have access. There are exclusions for old information, such as personal data about individuals who have been deceased for more than 10 years. Many obligations under the PDPA do not apply to 'business contact information', which refers to certain kinds of business-related information that an individual has not provided solely for personal purposes.

The PDPA does not prescribe different standards for sensitive personal data. However, PDPC guidance documents clarify that higher standards do apply to data such as national identification numbers and minors' personal data.

General obligations for data handlers

The PDPA contains 10 broad obligations that organisations must comply with in processing personal data:

1. Accountability Obligation: an organisation must implement the necessary policies and procedures to meet its obligations under the PDPA and must publish information about them.
2. Consent Obligation: an organisation must obtain the individual's consent before processing their personal data, unless an exception applies.
3. Purpose Limitation Obligation: an organisation may process personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual.
4. Notification Obligation: an organisation must notify the individual in advance of the purposes for which it intends to process their personal data.
5. Access and Correction Obligations: an organisation must, upon request, provide an individual with access to their personal data and correct errors or omissions in the personal data.
6. Accuracy Obligation: an organisation must make a reasonable effort to ensure that personal data is accurate and complete if it is likely to be used to make a decision that affects the individual or disclosed to another organisation.
7. Protection Obligation: an organisation must implement reasonable security arrangements to protect personal data in its possession or under its control.
8. Retention Limitation Obligation: an organisation must cease to retain personal data as soon as it is reasonable to assume that the purpose for which the personal data was collected is no longer being served by retention and retention is no longer necessary for legal or business purposes.
9. Transfer Limitation Obligation: an organisation must not transfer personal data outside Singapore unless certain conditions are satisfied.
10. Data Breach Notification Obligation: an organisation must assess whether a data breach is notifiable and make the requisite notifications.

An 11th obligation relating to data portability has yet to take effect.

Data subject rights

Individuals may request organisations for access to or correction of their personal data. Individuals may also withdraw consent to the processing of their personal data for any purpose. In certain circumstances, the organisation does not have to accede to a request: for example, where providing access would cause grave harm to the mental health of the requesting individual or would reveal personal data about another individual.

The PDPA frames these 'rights' as obligations of the organisation, rather than rights of the individual. In addition, some data subject rights recognised in other jurisdictions, such as the right to be forgotten and the right to object to automated decision-making, are not recognised in Singapore.

Specific regulatory areas

- Minors' personal data: minors' data protection is specifically addressed in PDPC guidance documents.[4] The general principle is that minors between 13 and 20 have sufficient understanding to give valid consent unless the organisation has reason to believe otherwise. Personal data of minors is considered to warrant higher standards of protection, especially when collected in a digital environment, in which age is less readily verifiable and children can easily access risky services without supervision.
- Biometric data: the use of biometric data in security applications is also the subject of detailed treatment in PDPC guidance.[5] The PDPC recommends that the use of security cameras be notified to individuals, even if the location is public and individuals would reasonably expect security cameras to be present. Biometric recognition systems, in turn, should be used for recognition and not identification, and should store as little personal data as possible.
- Employees' personal data: employee data does not benefit from higher standards of protection, nor is there express recognition of the imbalances in the employer/employee relationship in the context of consent. In addition, employers may sometimes process employees' personal data without consent, such as where processing is necessary for evaluating the employees' continued employment or suitability for promotion, for checking on employee conduct, or for managing employee benefits.

Technological innovation

- Cloud services: almost all organisations now utilise cloud service providers in their data processing workflow, especially for data storage. Singapore benefits from having several major providers host their servers here, including Amazon Web Services, Microsoft Azure, and Google Cloud. The involvement of cloud service providers raises issues relating to the identification and obligations of data intermediaries, which party is responsible for complying with cross-border transfer obligations, and third-party due diligence standards.
-

AI: organisations developing or deploying AI systems need to grapple with compliance relating to huge datasets and individuals with whom the organisation may not have a direct relationship. Such organisations may have to consider using processing bases other than consent, such as exceptions relating to business improvement, research, and legitimate interests. Such processing bases require more robust risk assessment procedures, and organisations will have to analyse whether the exceptions apply and keep records of their assessments.

- Healthcare: the Singapore government's vision of integrating technology into everyday life is quickly taking shape, facilitated by a relatively small population, high levels of technological adoption, and a substantial degree of government oversight. One proposed initiative is the consolidation of health information in a national database such that healthcare providers can access patients' history and patients can receive seamless care across providers. This initiative raises significant risks to sensitive information, and it will likely be subject to a separate, new law in addition to the PDPA.

International data transfer and data localisation

Under the PDPA, an organisation must not transfer any personal data out of Singapore unless it has first taken appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide to that personal data a standard of protection that is comparable to the protection under the PDPA. Legally enforceable obligations can be laws, contractual obligations, binding corporate rules, or any other legally binding instrument.

Singapore recognises the Asia Pacific Economic Co-operation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications. Any overseas recipient that is CBPR- or PRP-certified will be deemed to have met the requirements under the PDPA to receive personal data from Singapore.

Singapore encourages the use of the Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses and the PDPC's sample clauses for cross-border transfers. These are viewed as baseline clauses that should be adapted to each organisation's specific needs, and not pre-approved grounds for data transfers.

In respect of incoming data, the European Commission does not recognise Singapore as providing adequate protection for personal data. As a result, organisations need to implement appropriate safeguards before transferring personal data from the European Union to Singapore.

Company policies and practices

Corporate governance is viewed as key to ensuring that personal data protection is given sufficient weight in an organisation. Senior management is expected to be committed and involved. Organisations must appoint a data protection officer and make the officer's

business contact information available to the public. This information can also be voluntarily published on the companies' register.

Organisations must document and implement policies and procedures to meet their obligations under the PDPA. Information about such policies and procedures must be made publicly available. Key policies and procedures are: an online privacy policy, internal corporate privacy policy, complaints policy and processes, and data breach management policy and procedure. Risk assessments must also be documented, including data protection impact assessments and legitimate interest assessments.

The PDPC has also issued and expects organisations to comply with standards of practice for computer systems that process personal data. These standards focus on technological measures, such as code reviews, technical documentation, configuration standards, access controls, and password hygiene. While these standards are not enshrined in legislation, organisations that suffer data breaches may be directed to beef up their computer systems to meet these standards.

Organisations are encouraged to obtain the Data Protection Trustmark (DPTM) certification issued by the Singapore regulatory authorities. Obtaining cyber insurance and information security certifications like ISO/IEC 27001 and 27701 are also viewed favourably.

Discovery and disclosure

Any disclosure of data in response to government requests, court orders, or internal investigations will need to comply with requirements under the PDPA, including the requirement for a legitimate basis for disclosure. Such disclosures can be made without consent if one of the general exceptions applies, such as disclosures necessary in the vital interests of individuals or the national interest, or disclosures necessary for investigations or proceedings.

A disclosure of data out of Singapore must comply with the PDPA's requirements for cross-border data transfers, even if it can be legitimately made without the individual's consent. The discloser will, therefore, need to satisfy itself that the recipient will accord the individual's personal data a standard of protection comparable to that under the PDPA.

Public and private enforcement

Enforcement agencies

The Personal Data Protection Commission (PDPC) enforces the PDPA. Where a data breach also involves a criminal act, the police and state prosecutors may also be involved, and where a data breach touches a financial institution, the Monetary Authority of Singapore (MAS) may also be involved. The PDPC often works together with the police and the national cybersecurity agency to detect and address data breaches.

The PDPC has powers to direct alternative dispute resolution, review and investigate organisations' compliance with the PDPA, and issue directions and financial penalties. The PDPC does not typically initiate investigations unless it has received a complaint or an incident report. Where the PDPC receives a complaint best resolved between the organisation and the complainant, the PDPC may seek to facilitate an amicable resolution without exercising its powers of investigation. Where a complaint or incident reveals a broader issue or impacts multiple individuals, the PDPC may investigate instead. Investigations may culminate in a finding that there was no breach of the PDPA; or if there was a breach, the PDPC can issue directions to secure compliance and financial penalties.

Financial penalties for breach of the PDPA's personal data provisions are capped at SG$1 million or 10 per cent of the organisation's annual turnover in Singapore, whichever is higher. To date, the highest fine meted out is SG$750,000: a penalty imposed in 2019 on a technology vendor when health information in its care, including that of Singapore's then-prime minister Lee Hsien Loong, was exfiltrated in a cyberattack. Otherwise, fines have generally not exceeded SG$100,000.

Organisations may seek a reconsideration of the PDPC's decision, directions, or financial penalties, by making an application within 28 days. The PDPC will consider the organisations' submissions, and decide whether to affirm, revoke, or vary the contested decision.

Organisations may also appeal a decision, including a reconsidered decision, to the Data Protection Appeal Panel. The Appeal Panel will hear the appeal and may then remit the case back to the PDPC or make other decisions, such as varying the financial penalty or giving other directions. This can be appealed further to the High Court, and then to the apex Court of Appeal.

Recent enforcement cases

In early 2024, the PDPC issued a decision in respect of the Singapore-headquartered e-commerce platform Carousell.[6] Carousell operates an online marketplace for buying and selling new and second-hand goods and services. The decision covered two data breaches caused by system bugs: one, where Carousell's chat function automatically appended personal data to chat messages by mistake, and the second, where a threat actor scraped personal data using an API which was missing a filter and offered the data for sale. The breaches affected more than two million customers across several countries, and involved email addresses, telephone numbers, and birthdates.

The PDPC attributed both breaches to flawed technological processes. It found that Carousell had not conducted adequate pre-launch testing or code reviews for security issues, and that the organisation failed to adequately document the functional and technical specifications of its computer systems. According to the PDPC, Carousell could have avoided the system bugs or detected them much earlier if it had better processes in place.

Acknowledging Carousell's cooperation throughout the investigation process, its prompt remedial action, and that the threat actor in the second incident was particularly sophisticated in avoiding Carousell's security measures, the PDPC imposed a fine of SG$58,000 and directed Carousell to review and rectify its software testing procedures and processes for documenting software specifications.

The financial penalty meted out to Carousell was substantially lower than the fine imposed on homegrown cashback portal ShopBack in late 2023.[7] Hackers had breached ShopBack's servers using an access key with full administrative privileges, extracted its customer database, and listed it for sale on an online forum. The data included email addresses, bank account numbers, and partial credit card information, impacting a total of around 1.45 million users.

The PDPC found that ShopBack had breached its obligation to protect personal data, pointing out a lack of adequate processes for managing access keys, a failure to conduct periodic security reviews, and deficient incident management processes. ShopBack was fined SG$74,400.

These two cases garnered significant public attention. Carousell and ShopBack are well-known local startups that have become highly successful and are used by many Singaporeans. Several online commentators felt the companies were let off lightly and lamented the irreversible nature of the data breaches. At the same time, the cases highlighted the increasing sophistication of online threat actors and the active role the authorities are playing in detecting and mitigating such risks. Interestingly, Carousell only became aware of its second breach when it was alerted by the PDPC, which had seen the data on sale in the course of monitoring the dark web.

Private litigation

Individuals have the right to commence civil proceedings if they suffer loss or damage directly as a result of an organisation's breach of the PDPA. Such proceedings have to be brought as a court action, because the court can award any relief it thinks fit, including damages and injunctions, whereas the PDPC lacks such powers.

Only one civil case has been brought in the history of the PDPA.[8] Michael Reed was a customer of Alex Bellingham's former employers, a fund management group. When Bellingham moved to a new firm, he contacted Reed using Reed's personal email address, citing Reed's investment activities. Reed sued Bellingham for emotional distress caused by the unauthorised collection and use of his personal data, and loss of control of his personal data.

The action was commenced in the District Court, which granted Reed an injunction against Bellingham's further processing of Reed's personal data and ordered Bellingham to destroy the data in his possession. Bellingham appealed to the High Court, which set aside the District Court's judgment, holding that Reed's emotional distress and loss of control of his personal data did not constitute the requisite loss or damage for the purpose of a private action.

Reed appealed to the Court of Appeal. The apex court disagreed with the High Court, holding that while loss of control of personal data did not constitute the requisite loss or damage (because it would happen in every case of breach), emotional distress did. Given that Bellingham's breach involved sensitive financial data, that he refused to assure Reed that he would protect the personal data, and that Reed's behaviour demonstrated anxiety over the misuse of his personal data, the Court of Appeal found that Reed had suffered a loss or damage entitling him to civil relief. The District Court's orders were restored in full.

While this case clarified the scope of the right of private action, it also raises questions as to how the average member of the public might exercise this right effectively. To begin with, the cost of a court action may put an individual off bringing a case, especially if the defendant is a company with deep pockets. Moreover, the evidential burden of proving actual emotional distress may be high, especially since individuals may respond to distressful situations in different ways. Finally, since Reed did not seek damages, the case does not give potential plaintiffs guidance on how a court would quantify damages.

Considerations for foreign organisations

All organisations that process personal data in Singapore are subject to the PDPA, regardless of whether the organisation is located in Singapore. Processing personal data in Singapore could mean collecting personal data from individuals located in Singapore, storing personal data on servers hosted in Singapore, or disclosing personal data to recipients located in Singapore.

Organisations located outside Singapore that process personal data in Singapore should consider storing the data with the major cloud service providers that host their servers here, such as Amazon Web Services, Microsoft Azure, and Google Cloud. This minimises the compliance burden in respect of cross-border transfers. Many organisations operating in South-East Asian countries also choose to consolidate their data in Singapore due to practical considerations like the ease of doing business and communication, strong infrastructure, and robust legal system.

Cybersecurity and data breaches

Cybersecurity has been an important topic in Singapore in the past few years. A 2023 report[9] found that Singapore systems suffered 32 million cyberattacks in the previous year, a 20 per cent year-on-year increase. This was much higher than the regional average for countries in the Asia-Pacific. Cyberattacks have been reported on reputable businesses such as the Jumbo restaurant chain and the SingHealth hospital group. In 2024, a Russian media outlet leaked an audio recording of a confidential online call between senior German military officials, one of whom had dialled in over an unsecured Internet connection while in Singapore for the Singapore Airshow.

The Cybersecurity Act 2018 (CSA) is the cornerstone of Singapore's cybersecurity regime and is complemented by the Computer Misuse Act 1993 (CMA).

The CSA establishes a framework for protecting Critical Information Infrastructure (CII), which are computer systems critical to the provision of essential services like healthcare, finance, and utilities designated by the Cyber Security Agency. CII owners must conduct risk assessments to identify vulnerabilities in their systems, implement appropriate security measures, promptly report cybersecurity incidents, cooperate with investigations, and take remedial actions as directed by the Cyber Security Agency.

The CSA also regulates cybersecurity service providers to ensure they offer high-quality services. All cybersecurity service providers must be licensed and comply with their

licence conditions, including keeping records of all their engagements and disclosing those records to the authority upon request.

Non-compliance with the CSA may result in penalties, including fines, criminal prosecutions, and the revocation or suspension of licences. In addition to enforcing the CSA, the Cyber Security Agency takes proactive measures to prevent, detect, and respond to cybersecurity threats and incidents. It issues advisories to protect stakeholders from vulnerabilities, conducts awareness programmes, promotes good cyber hygiene practices, and partners with industry to encourage innovation and train skilled professionals.

In May 2024, Singapore lawmakers approved updates to the CSA to expand its reach. CII owners will soon need to report more types of incidents, including those that occur in their supply chains, to address new cyber threats. In addition to CII, the authorities will now also regulate Systems of Temporary Cybersecurity Concern (those which are temporarily at high risk, such as at international summits – the Shangri-La defence dialogue and the Singapore Airshow being two examples), Entities of Special Cyber Security Interest (which may hold sensitive information or perform a function of national interest, although not to the degree of CII) and Foundational Digital Infrastructure service providers (such as cloud service and data centre providers). These changes have yet to take effect.

While the CSA focuses on defence against cybersecurity threats, the CMA deals with the prosecution of cybercriminals. Offences under the CMA include hacking, unauthorised data modification, using a computer to commit a crime, and interfering with computer systems (such as through denial-of-service attacks). A person can be guilty of an offence even if they committed it while outside Singapore.

Financial institutions regulated by the Monetary Authority of Singapore (MAS), including insurers, banks, and credit card companies, are also subject to stringent cybersecurity requirements.[10] These include obligations to assess risks posed by technology service providers, to establish incident response plans, and to implement security safeguards and business continuity plans. The MAS has stepped up enforcement against errant financial institutions, escalated by a phishing scam in late 2021 targeting the Overseas Chinese Banking Corporation (OCBC) and resulting in customer losses of more than US$6 million.

Apart from the high cybersecurity standards imposed on systems of national interest and financial institutions, the law does not mandate cybersecurity compliance for businesses in general. However, the Cyber Security Agency encourages firms to obtain certifications such as ISO information security certifications and the local Cyber Essentials and Cyber Trust certifications, to boost cyber hygiene and consumer trust. In addition, organisations still have to comply with the PDPA, so they could incur liability if a cybersecurity incident results in a breach of personal data.

Software development and vulnerabilities

The PDPC sets out best-practice standards for software development in the context of personal data protection.[11] It deals with coding issues (testing scenarios, code reviews, documentation), configuration issues (security protocols, firewalls, access controls, code management), and emphasises the need for data protection by design and by default.

The Cyber Security Agency has also set standards to promote good software development practices. For example, it has published a Safe App Standard, a security benchmark for developers whose apps perform high-risk transactions. It has also endorsed the Guidelines for Secure AI System Development, which contains recommendations developed by the United Kingdom National Cyber Security Centre to help providers of AI systems establish data-secure products.

Digital governance and convergence with competition policy

Singapore does not have a law specifically targeting competition in the digital market. It relies on its existing competition law, broadcasting law, and data protection frameworks, reflecting a view that existing legal structures are sufficient to deal with issues arising in data-driven industries.

Nevertheless, the authorities recognise that companies which hold substantial user data or provide popular online services must maintain high security standards. They have not shied away from reprimanding dominant technology players for cybersecurity lapses – in early 2024, a minister of state publicly called out Meta for refusing to implement safety features recommended by the authorities. From mid-2024, platforms like Facebook, Instagram, and WhatsApp will be required to roll out verification measures in a bid to reduce online crime.

Outlook and conclusions

In a rapidly evolving digital world, Singapore's data protection and cybersecurity landscape is poised for continued development. Cyberattacks and scams are likely to keep increasing, as more aspects of peoples' lives go digital and criminals find more opportunities to profit. Technological advancements will allow businesses to process huge amounts of personal data in new ways.

Regulators will need to keep up. The Singapore government is staying abreast, with the 2024 amendments to the Cybersecurity Act and the proposed new health information law highlighting a recognition of new cyberthreats and the risks and potentials associated with increasing reliance on digital systems. In the coming months, the authorities will need to consider whether AI-specific laws need to be enacted to deal with advanced AI systems, whether a firmer hand is needed to ensure businesses adequately protect personal data, and how to strike the best balance between facilitating business goals and protecting individuals' data.

Endnotes

1 https://www.pdpc.gov.sg/help-and-resources/2020/04/enquiry-and-complaint-figures. ^ Back to section

2 https://www.straitstimes.com/opinion/widespread-adoption-of-ai-is-a-national-priority. ^ Back to section

3 https://www.channelnewsasia.com/singapore/cyber-crime-digital-fraud-attack-bots-lexisnexis-report-3992166. ^ Back to section

4 Chapter 8 of the Advisory Guidelines for Selected Topics; Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment. ^ Back to section

5 PDPC Guide on Responsible Use of Biometric Data in Security Applications; Chapter 4 of the Advisory Guidelines for Selected Topics. ^ Back to section

6 Breach of the Protection Obligation by Carousell [2023] SGPDPC 13. ^ Back to section

7 E-commerce Enablers Pte. Ltd. [2023] SGPDPC 6. ^ Back to section

8 *Reed, Michael v Bellingham, Alex* (Attorney-General, intervener) [2022] SGCA 60. ^ Back to section

9 LexisNexis Risk Solutions APAC Cybercrime Report 2023. ^ Back to section

10 MAS Technology Risk Management Guidelines and Notices; MAS Cyber Hygiene Notices. ^ Back to section

11 PDPC Handbook on How to Guard Against Common Types of Data Breaches; PDPC Checklists to Guard Against Common Types of Data Breaches. ^ Back to section

AMICA LAW LLC

Anna Toh anna.toh@amicalaw.com

Amica Law LLC