GDR

INSIGHT HANDBOOK
2024

The GDR *Insight Handbook 2024* delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

Singapore: International Agreements Boost Cyber Defence

Lim Chong Kin and Anastasia Su-Anne Chen
Drew & Napier LLC

Key statutes, regulations and adopted international standards

The Cybersecurity Act

The Cybersecurity Act 2018 (the Cybersecurity Act) is the principal legislation dedicated to cybersecurity in Singapore. The primary objective of the Cybersecurity Act is to provide the necessary legislative framework to better protect critical information infrastructure (CII), and to give the Cybersecurity Agency of Singapore (CSA) the powers required to act on cybersecurity incidents that impact Singapore.

The Commissioner of Cybersecurity (the Commissioner) may designate a computer or computer system a CII if they are satisfied that:

- it is a computer or a computer system necessary for the continuous delivery of an essential service, the loss or compromise of which will have a debilitating effect on the availability of essential services in Singapore; and
- the computer or computer system is located wholly or partly in Singapore.

The essential services identified under the First Schedule of the Cybersecurity Act are services relating to the following sectors: energy; info-communications; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; government; and media.

The Cybersecurity Act is accompanied by:

- the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (the CII Regulations);
- the Cybersecurity (Confidential Treatment of Information) Regulations 2018 (the Confidentiality Regulations);

- the Cybersecurity (Cybersecurity Service Providers) Regulations 2022; and
- the Cybersecurity (Composition of Offences) Regulations 2022.

The Commissioner has also issued a second edition of the Cybersecurity Code of Practice for Critical Information Infrastructure (the Cybersecurity Code), with effect from 4 July 2022. The Cybersecurity Code is intended to specify the minimum protection policies that a CII owner shall implement to ensure the cybersecurity of its CII. Subject to exceptions, a CII owner must comply with the Cybersecurity Code under section 11(6) of the Cybersecurity Act. Some of the obligations in the Cybersecurity Code include the requirement for the CII owner to establish, in writing, a cybersecurity risk management framework, as well as a cybersecurity incident response plan and crisis communication plan. CII owners must also develop a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) to ensure that the CII can continue to deliver essential services in the event of disruptions due to a cybersecurity incident.

Other legislation

Aside from the Cybersecurity Act, other key legislation includes the Personal Data Protection Act 2012 (PDPA) and the Computer Misuse Act 1993 (CMA).

Under the PDPA, organisations are required to make reasonable security arrangements to protect personal data in their possession or under their control to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks and to prevent the loss of any storage medium or device on which personal data is stored (the protection obligation).[1]

Under the CMA, certain cyber activities are criminalised. These include hacking, denial-of-service attacks or infecting computer systems with malware, as well as the possession or use of hardware, software or other tools to commit offences, and other acts preparatory to or in furtherance of the commission of any offence.

In addition to the PDPA and the CMA, there are also sector-specific frameworks that have requirements relating to cybersecurity issues. For example:

- The telecommunications and media regulator, the Infocomm Media Development Authority (IMDA), has issued the Telecommunications Cybersecurity Code of Practice (the Telecommunications Code), which internet service providers in Singapore are required to comply with. The Telecommunications Code includes requirements relating to security incident management, including the prevention, protection, detection of, and response to, cybersecurity threats. The Telecommunications Code was based

1 Personal Data Protection Act 2012 (PDPA), section 24.

on international standards and best practices, including ISO/IEC[2] 27011 and the IETF[3] Best Current Practices.

- Regarding the financial sector, the Monetary Authority of Singapore (MAS), Singapore's central bank and financial regulatory authority, has issued data protection-related regulatory instruments – such as the MAS Notices and Guidelines on Technology Risk Management, the Notices on Cyber Hygiene and the Guidelines on Outsourcing – which require financial institutions, among other things, to notify the MAS of breaches of security and confidentiality of customer information.

International standards

The Singapore Common Criteria Scheme (SCCS) is a certification scheme that provides a cost-effective regime for the info-communications industry to evaluate and certify their information technology (IT) products. The SCCS is based on the international standard ISO/IEC 15408, which is also known as the Common Criteria for Information Technology Security Evaluation, or the Common Criteria.

Regulatory bodies

Enforcement of the Cybersecurity Act

The CSA is the regulatory body responsible for enforcing the Cybersecurity Act. It provides dedicated and centralised oversight of national cybersecurity functions to protect essential services. It is also responsible for the holistic development of Singapore's cybersecurity landscape. The CSA comes under the purview of the Prime Minister's Office and the Ministry of Communications and Information.

The CSA is headed by the Commissioner, who is also the chief executive of the CSA. Assistant commissioners may also be appointed to assist the Commissioner. The CSA works closely with sector regulators as they are best placed to understand the unique context and complexity of their sectors and can provide advice on the necessary requirements.

2 International Organisation for Standardisation/International Electrotechnical Commission.
3 Internet Engineering Task Force.

The relevant powers prescribed to the Commissioner to aid them in the enforcement of the Cybersecurity Act include:

- the power to obtain information to ascertain whether a computer or computer system fulfils the criteria or the cybersecurity obligations of CIIs;[4]
- the power to issue written directions to the CII owners to ensure the cybersecurity of the CII or the effective administration of the Cybersecurity Act;[5]
- the power to investigate cybersecurity threats or incidents, including those involving non-CII. The Commissioner may exercise powers with varying levels of intrusiveness, depending on the severity of the threat or incident;[6] and
- the power to authorise an officer to conduct investigations in relation to any offence under the Cybersecurity Act.[7]

At the time of writing, the CSA has not published any reports of significant enforcement actions under the Cybersecurity Act.

Enforcement of other legislation

The Singapore Police Force, working together with the Public Prosecutor, is generally responsible for investigating and prosecuting cybercrimes under the CMA.

The data protection authority, the Personal Data Protection Commission (PDPC), is responsible for enforcing the PDPA. Where an organisation fails to comply with the protection obligation under the PDPA, the PDPC may impose a financial penalty of up to S$1 million or 10 per cent of the organisation's annual turnover in Singapore, whichever is higher. The PDPC may also impose such directions as it thinks fit on the organisation under the circumstances to ensure compliance with the protection obligation.

Sector regulators such as the IMDA and the MAS are responsible for enforcing their individual sector-specific frameworks.

4 Cybersecurity Act, sections 8 and 10.
5 Cybersecurity Act, section 12.
6 Cybersecurity Act, sections 19 and 20.
7 Cybersecurity Act, sections 38 and 39.

Relevant company obligations to protect against cyber threats

Under the Cybersecurity Act, owners of CII must comply with a number of general obligations, including:

- compliance with notices issued by the Commissioner to furnish information relating to the CII;[8]
- compliance with codes of practice, standards of performance and written directions in relation to the CII as may be issued by the Commissioner, such as the Cybersecurity Code;[9]
- notifying the Commissioner of any change in ownership of the CII;[10]
- notifying the Commissioner of any prescribed cybersecurity incidents relating to the CII;[11]
- regularly auditing the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance. The audits must be carried out by an auditor approved or appointed by the Commissioner;[12]
- carrying out regular cybersecurity risk assessments of the CII;[13] and
- participating in cybersecurity exercises as required by the Commissioner.[14]

The details of those obligations may be specified in the Cybersecurity Code. The CSA will periodically introduce supplementary references to help CII owners comply with the Cybersecurity Code. This includes the Security-by-Design Framework, which was developed to guide CII owners through the process of incorporating security into their systems development life cycle. Security-by-design is an approach that addresses the cyber protection considerations throughout a system's life cycle and is one of the key components of the Cybersecurity Code.

With regard to the protection of personal data, organisations are required to comply with the protection obligation under the PDPA in respect of the personal data in their possession or control, as mentioned above.

The PDPC has issued various advisory guidelines and guides. For example, the Advisory Guidelines on Key Concepts in the PDPA sets out a number of administrative, physical and technical security arrangements that organisations may consider adopting. The PDPC also released the Guide to Data Protection by Design for ICT Systems, which recommends basic and enhanced practices

8 Cybersecurity Act, section 10.
9 Cybersecurity Act, sections 11 and 12.
10 Cybersecurity Act, section 13.
11 Cybersecurity Act, section 14.
12 Cybersecurity Act, section 5.
13 Cybersecurity Act, section 15.
14 Cybersecurity Act, section 16.

that organisations can incorporate into their technology policies, systems and processes.

For the financial sector, the MAS Notice on Technology Risk Management imposes requirements on financial institutions to establish frameworks and processes for the identification of critical systems, and implement IT controls to protect customer information from unauthorised access or disclosure. Examples of critical systems include automated teller machine (ATM) systems, online banking systems, and systems that support payment, clearing or settlement functions.

The effect of local laws on foreign businesses

Under certain circumstances, the Cybersecurity Act and PDPA may be applicable to foreign businesses in Singapore.

As mentioned above, a computer or computer system located wholly or partly in Singapore may be designated as a CII for the purposes of the Cybersecurity Act.[15] As such, foreign businesses that are owners of such CII must comply with the relevant requirements of the Cybersecurity Act, as set out in the section above on 'Relevant obligations for companies to protect against cyber threats'.

Subject to its detailed scope,[16] the data protection provisions under the PDPA apply to all organisations (and persons) that are not public agencies (including those not formed or recognised under the laws of Singapore or without residency, an office or a place of business in Singapore).[17] As such, the data protection provisions under the PDPA (including the protection obligation) may be applicable to foreign businesses that carry out activities involving personal data in Singapore.

In comparison, the CMA provides that the provisions of the CMA shall have effect, in relation to any person, whatever their nationality or citizenship, outside as well as within Singapore. Where an offence under the CMA is committed by any person in any place outside Singapore, they may be dealt with as if the offence had been committed within Singapore.[18]

Subject to certain circumstances, the CMA will apply if: (1) the accused was in Singapore at the material time; (2) the computer, program or data was in Singapore at the material time; or (3) the offence causes, or creates a significant risk of, serious harm in Singapore.[19] Examples of acts that seriously diminish

15 Cybersecurity Act, section 7.
16 For more detail, see the chapter on 'Singapore: Privacy'.
17 PDPA, section 2(1).
18 Computer Misuse Act 1993 (CMA), section 13(1)–(2).
19 CMA, section 13(3).

or create a significant risk of seriously diminishing public confidence in the provision of an essential service (ie, significant harm) include:

- publication to the public of the medical records of patients of a hospital in Singapore; and
- providing public access to the account numbers of customers of a bank in Singapore.

Directors' responsibilities

Under the Cybersecurity Act, personal liability is imposed on officers, members (if the members of a corporation manage its affairs) and individuals involved in a corporation's management and in a position to influence its conduct for offences committed by the corporation under the Cybersecurity Act, if they:

- consented, connived or conspired with others to bring about the offence;
- were knowingly concerned or party to the commission of the offence; or
- knew or ought reasonably to have known that the offence by the corporation would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence.[20]

Regarding offences committed by an unincorporated association or a partnership under the Cybersecurity Act, personal liability is imposed on officers of unincorporated associations and members of their governing bodies, partners in a partnership, and individuals involved in the management of the unincorporated association or partnership and who are in a position to influence its conduct, in circumstances similar to those set out in the preceding paragraph.[21]

Moreover, a director's failure to adequately manage an organisation's cybersecurity arrangements may amount to a breach of their directors' duties, for example, under section 157 of the Companies Act 1967, which requires a director to use reasonable diligence in the discharge of the duties of their office.

Best practices for responding to data breaches

Cybersecurity incidents

The owner of CII must notify the Commissioner of:

- a prescribed cybersecurity incident in respect of the CII;

20 Cybersecurity Act, section 36.
21 Cybersecurity Act, section 37.

- a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with CII; and
- any other type of cybersecurity incident in respect of CII that the Commissioner has specified by written direction to the owner.[22]

Details of the cybersecurity incident must be notified to the Commissioner within two hours of becoming aware of the occurrence and, within 14 days of the initial notification, the following supplementary details must be provided:

- the cause of the cybersecurity incident and its impact on the CII, or any interconnected computer or computer system; and
- the remedial measures that have been taken.[23]

The prescribed cybersecurity incidents mentioned above are:

- the unauthorised hacking of CII;
- the installation or execution of unauthorised software or computer code of a malicious nature on CII;
- any man-in-the-middle attack, session hijack or other unauthorised interception of communication between CII and an authorised user; and
- any denial-of-service attacks that adversely affect the availability or operability of CII.[24]

Further, the Singapore Computer Emergency Response Team (SingCert) publishes alerts, advisories and recommendations detailing procedures or mitigation measures for organisations to respond to new cybersecurity threats. SingCert is set up by the CSA and facilitates the detection, resolution and prevention of cybersecurity-related incidents on the internet.

Data breaches

Recent amendments to the PDPA introduced a mandatory data breach notification regime. Under the new data breach notification obligation (Part 6A of the PDPA), in the event of a data breach, organisations are required to conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is notifiable.

22 Cybersecurity Act, section 14.
23 Cybersecurity (Critical Information Infrastructure) Regulations 2018 (the CII Regulations), Regulation 5.
24 CII Regulations, Regulation 5.

A data breach is a 'notifiable data breach' if it:

- results in, or is likely to result in, significant harm to any individual to whom any personal data affected by a data breach relates; or
- is, or is likely to be, of a significant scale (ie, 500 or more individuals).

The organisation must notify the PDPC of the notifiable data breach as soon as practicable, but in any case, no later than three calendar days after making the determination that a data breach is a notifiable data breach. A data intermediary must, without undue delay, notify the primary organisation (or public agency) on whose behalf it is processing personal data when it has reason to believe that a data breach has occurred in relation to personal data that it is processing on the latter's behalf.

Subject to certain prescribed exceptions, on or after notifying the PDPC, organisations must also notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals.

The Personal Data Protection (Notification of Data Breaches) Regulations 2021 set out further prescribed requirements relating to the data breach notification obligation, including the contents of the notification to the PDPC as well as the categories of prescribed personal data that are deemed to result in significant harm to the affected individual.

Where criminal activity is suspected, the PDPC recommends that organisations notify the police so that they may offer assistance in containing the breach and preserve evidence for investigation.

Organisations must also notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals to whom the information relates. There are two exceptions to this requirement to notify affected individuals, namely:

- where organisations have taken actions in accordance with any prescribed requirements that render it unlikely that the breach will result in significant harm to affected individuals; and
- where the personal data that was compromised by the data breach is subject to technological protection (eg, encryption) such that the data breach is unlikely to result in significant harm to the affected individuals.

Organisations must also not notify affected individuals if instructed by a prescribed law enforcement agency or directed as such by the PDPC, for example, in circumstances where the notification may compromise investigations or prejudice enforcement efforts.

For more information, organisations may refer to the PDPC's Guide on Managing and Notifying Data Breaches under the PDPA.

Breaches in the financial sector

With respect to the financial sector, the MAS Notice on Technology Risk Management (the TRM Notice) requires financial institutions to notify MAS as soon as possible, but no later than an hour, upon the discovery of a relevant IT incident.[25] The TRM Notice also requires financial institutions to submit a root cause and impact analysis report to MAS within 14 days, or a longer period as MAS may allow, from the discovery of the relevant IT incident.[26]

Private redress options for unauthorised cyber activity

The Cybersecurity Act does not provide for parties to seek private redress for unauthorised cyber activity or failure to adequately protect systems and data.

In contrast, under the PDPA, any individual who suffers loss or damage directly as a result of an organisation's breach of the PDPA has a right of private action for relief in civil proceedings in court.[27] If the PDPC has made a decision under the PDPA in respect of the same breach, this right is only exercisable after the PDPC's decision has become final as a result of there being no further right of appeal.

The Criminal Procedure Code 2010 provides that, after a person is convicted of any offence, the court must consider whether to make an order for the payment of compensation to the person injured (in respect of their person, character or property) by the relevant offences;[28] therefore, should an individual be convicted of a cybercrime under the CMA, the court may also order compensation to any other person who has suffered injury as a result of that offence.

Individuals may also bring private claims under common law, such as the laws of contract or the tort of negligence.

25 An IT security incident means an event that involves a security breach, such as hacking of, intrusion into or denial-of-service attack on a critical system, or a system, which compromises the security, integrity or confidentiality of customer information.

26 A relevant incident generally means a system malfunction or IT security system, which has a severe and widespread impact on the financial institution's operations or materially impacts its services to its customers.

27 PDPA, section 480.

28 Criminal Procedure Code 2010, section 359.

Updates and trends

Singapore has been increasingly paying attention to cybersecurity issues over the past few years.

To strengthen Singapore's operational cybersecurity capabilities, the government has signed a number of memorandums of understanding (MOUs) with other countries to increase cybersecurity cooperation in key areas such as information exchange and sharing on cyber threats and cyberattacks and development of cybersecurity standards, as well as to collaborate on regional cybersecurity capacity building. Singapore has signed MOUs with Australia, Canada, France, India, South Korea, the Netherlands, the UK and the US.

In addition, Singapore has signed a Joint Declaration on Cybersecurity Cooperation with Germany and a memorandum of cooperation on Cybersecurity with Japan. Further, the CSA and the National Cyber Policy Office of New Zealand signed a formal arrangement to strengthen cybersecurity cooperation between both countries.

On 21 June 2023, the CSA and the National Cybersecurity Agency (NCSA) of Qatar signed an MOU for cooperation in the field of cybersecurity. The MOU will facilitate information sharing between both sides' computer emergency response teams, exchanges to better secure industrial control systems and operating technology widely used in CII systems, and collaboration on mutual areas of national interest. Further areas of potential cooperation include research, cybersecurity education and training, and partnership on national initiatives of mutual interest. This will strengthen both countries' ability to address and tackle the transnational challenge of cybersecurity.

In addition to MOUs, on 6 October 2020, Singapore's Deputy Prime Minister launched Singapore's Safe Cyberspace Masterplan 2020, which outlines a blueprint for the creation of a safer and more secure cyberspace in Singapore. It was developed in consultation with industry and academic partners and aims to raise the general level of cybersecurity for individuals, communities, enterprises and organisations. It comprises three strategic prongs:

- securing Singapore's core digital infrastructure;
- safeguarding Singapore's cyberspace activities; and
- empowering Singapore's cyber-savvy population.

Singapore has also sought to build strategic partnerships with the industry. On 3 October 2019, the CSA and FireEye, Inc announced their anticipated expanded scope of their strategic partnership within areas of cybersecurity capability development and research and development. In an MOU signed by the two parties, the organisations articulated their intention to extend the

framework of their cybersecurity cooperation to include capability building and the sharing of threat information.

Separately, in August 2021, the Government Technology Agency (GovTech) launched a new Vulnerability Rewards Programme (VRP) on top of the existing Government Bug Bounty Programme and the Vulnerability Disclosure Programme. The VRP offers monetary rewards ranging from US$250 to US$5,000 to registered and authorised hackers, depending on the severity of the vulnerabilities discovered.

On 29 March 2022, the CSA launched a new cybersecurity certification programme to recognise enterprises that have adopted and implemented good cybersecurity practices, comprising two cybersecurity marks: Cyber Essentials and Cyber Trust. Cyber Essentials recognises enterprises that have put in place cyber hygiene measures, while Cyber Trust is a mark of distinction that recognises enterprises with comprehensive cybersecurity measures and practices.

On 29 April 2022, the CSA published the Guidelines for CII Owners to Enhance Cyber Security for 5G Use Cases (Guidelines for 5G Use Cases) to address challenges in the 5G era. Although not binding, the Guidelines for 5G Use Cases provides insightful guidance to CII owners on identifying potential risks and threats. Additionally, the guidelines provide recommendations on how the potential risks of such threats can be mitigated.

On 20 October 2022, it was announced that the CSA and Germany's Federal Office for Information Security (BSI) will sign a Mutual Recognition Arrangement (MRA) on the cybersecurity labels to be issued for consumer smart products. The CSA's Cybersecurity Labelling Scheme (CLS) is the first multi-level labelling scheme in the Asia-Pacific region. Under the scheme, smart devices are rated according to their levels of cybersecurity provisions, from Level 1 to Level 4. With the MRA in place, smart consumer products issued with Germany's IT Security Label and Singapore's Cybersecurity Label will be mutually recognised in either country. Products issued with the BSI's label will be recognised by the CSA to have fulfilled CLS Level 2 requirements, while products with CLS Level 2 and above will be recognised by BSI.

Also in 2022, the Singapore government convened the inter-agency Counter Ransomware Task Force (CRTF) to develop and make recommendations on possible policies, operational plans and capabilities to improve Singapore's counter ransomware efforts. The CRTF comprises senior government representatives from the technology, cybersecurity, financial regulation and law enforcement domains whose mandate is to develop and make recommendations on countering ransomware. The CRTF published its first report on November 2022, setting out its findings and recommendations for the government to effectively deter and secure Singapore from ransomware attacks.

Legislative updates

Part 5 and the Second Schedule of the Cybersecurity Act, which relate to the licensing framework for cybersecurity services providers comprising managed security operations centre monitoring services and penetration testing services, came into effect on 11 April 2022. The Cybersecurity (Cybersecurity Service Providers) Regulations 2022 and the Cybersecurity (Composition of Offences) Regulations 2022 also became operative from 11 April 2022.

Currently, only penetration testing services and managed security operations centre monitoring services are prescribed as licensable cybersecurity services under the Cybersecurity Act. Any person who engages in the business of providing any licensable cybersecurity services to another person without a licence after 11 October 2022 shall be guilty of an offence and liable on conviction to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding two years.[29]

On 11 April 2022, the CSA also set up the Cybersecurity Services Regulation Office (CSRO). The functions of the CSRO include:

- enforcing the licensing framework, for example, managing licensing processes, and imposing and enforcing licence conditions;
- responding to queries and feedback from licensees, businesses and the public; and
- developing and sharing resources on licensable cybersecurity services with consumers such as the list of licensees.

The published list of licensed service providers may be accessed on the CSRO's website.[30]

As at the time of writing, the Cybersecurity Act is under review. In particular, the CSA is looking to expand the Cybersecurity Act to improve awareness of threats over Singapore's cyberspace and protect virtual assets (eg, systems hosted on the cloud) as CII if they support essential services. Beyond the CIIs, the review will also cover foundational digital infrastructure and key digital services, such as apps, that are important to sustain Singapore's reliance on digital infrastructure and services.

On 4 July 2022, the revised Cybersecurity Code came into effect. The Cybersecurity Code was revised to:

- improve the odds of defenders against threat actors' sophisticated tactics, techniques and procedures and impede the attacks;

29 Cybersecurity Act, section 24(2).
30 Cybersecurity Services Regulation Office, 'Licensed Service Providers'.

- enhance agility in addressing emerging risks in specific domains (eg, Cloud, 5G and artificial intelligence); and
- enable coordinated defences between the government and private sectors to identify, discover and respond to cybersecurity threats and attacks on a timely basis.

Separately, the Personal Data Protection (Amendment) Act 2020 was passed by the Singapore parliament on 14 November 2020, and most of the amendments to the PDPA have come into effect.

Case study

On 14 January 2019, the PDPC imposed its highest financial penalties to date of S$250,000 and S$750,000, respectively, on Singapore Health Services Pte Ltd (SingHealth) and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA. This unprecedented data breach, which arose from a cyberattack on SingHealth's patient database system, caused the personal data of some 1.5 million patients and the outpatient prescriptions of nearly 160,000 patients to be compromised.

Lim Chong Kin
Drew & Napier LLC

Lim Chong Kin is the managing director of Drew & Napier's corporate and finance department. He heads the telecommunications, media and technology (TMT) and competition, consumer and regulatory practices, and is co-head of the data protection, privacy and cybersecurity practice.

Chong Kin is cited by many publications as a leading lawyer in the fields of TMT, and regulatory, antitrust and competition. He is highly regarded by his peers, clients and rivals for his expertise and is lauded for being a 'very technically proficient and commercially savvy lawyer', who has 'unique insights into policy direction and interpretation' and 'understands regulatory thinking like no other lawyer in the field'.

Chong Kin acts for various clients, including household-name technology companies, payment systems providers, cloud service providers, media conglomerates, telecommunication providers and e-commerce start-ups. His broad experience includes supporting regulators to develop first-of-their-kind regulatory frameworks. He has acted as external counsel to the then Infocomm Development Authority in liberalising the telecoms industry and developing the Telecom Competition Code, and the then Media Development Authority in

developing the Media Market Conduct Code. He has also supported the Personal Data Protection Commission in numerous projects to administer the Personal Data Protection Act 2012. Chong Kin continues to advise clients in cutting-edge ICT, data protection and cybersecurity matters.

Anastasia Su-Anne Chen

Drew & Napier LLC

Anastasia Su-Anne Chen is a director in Drew & Napier's corporate and finance department. Her key areas of practice are data protection, privacy, cybersecurity, and technology, media, and telecommunications (TMT).

Before joining the firm, Anastasia was deputy chief counsel to Singapore's Personal Data Protection Commission (PDPC) and Infocomm Media Development Authority (IMDA) for over nine years. She was lead counsel for PDPC's matters, IMDA's procurement and IP portfolios, as well as the legal adviser to IMDA's Data Administration Group. This included advising on the administration, application and enforcement of Singapore's Personal Data Protection Act 2012 (PDPA).

Significant national projects that she has worked on include the amendments to the PDPA, which came into effect on 1 February 2021, and Singapore's participation and implementation of the APEC Cross Border Privacy Rules System.

Anastasia has broad experience in data protection compliance programmes and documentation, cross-border data transfers, the coordination of multi-jurisdictional projects and data breach management. She also advises on related TMT matters, such as regulatory issues in respect of data centres and the use of artificial intelligence.

DREW & NAPIER

Drew & Napier's work in data protection, privacy and cybersecurity precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. Our expertise extends beyond general data protection law to sectoral frameworks, in particular, in the telecommunications, media and technology; financial; and healthcare sectors. Over the past decade, Drew & Napier has been one of the leading practices in this field, having worked on a number of important matters for our clients.

We have been at the forefront of data protection laws in Singapore, given that we were involved with the Infocomm Media Development Authority and Personal Data Protection Commission (IMDA/PDPC) in setting up the implementing data protection laws in Singapore. We continue to represent the IMDA/PDPC in advisory, enforcement and policy work.

We also regularly act for a wide range of clients on a variety of data protection matters, including the implementation of group-wide data protection compliance programmes, the localisation of global data privacy policies, data protection training programmes, advising companies on dealing with data breaches, conducting regulatory risk audits, and addressing ad hoc queries.

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315
Tel: +65 6531 4110
Fax: +65 6535 4864

www.drewnapier.com

Lim Chong Kin
chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen
anastasia.chen@drewnapier.com