GDR INSIGHT

HANDBOOK 2021

HANDBOOK
2021

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-266-4

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Privacy

Cybersecurity

Data in practice

PREFACE

Global Data Review is delighted to publish this second edition of the *GDR Insight Handbook*.

The handbook 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 legislation that a ects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of arti cial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell datasets, and the intersection of privacy, data and antitrust. A chapter is dedicated to the use of arti cial intelligence in cross-border forensic investigations.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at November 2020. Although every e ort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing eld of practice, and therefore speci c legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
November 2020

PART 2

Cybersecurity

SINGAPORE: CYBERSECURITY

Lim Chong Kin and Charis Seow
Drew & Napier LLC

Key statutes, regulations and adopted international standards

The Cybersecurity Act

The Cybersecurity Act 2018 (No. 9 of 2018) (the Cybersecurity Act) is the principal legislation dedicated to cybersecurity in Singapore. The primary objective of the Cybersecurity Act aims to provide the necessary legislative framework to better protect critical information infrastructure (CII), and to give 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 he is 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 the 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) and Cybersecurity (Confidential Treatment of Information) Regulations 2018 (the Confidentiality Regulations).

In addition, the Commissioner has also issued the Cybersecurity Code of Practice for Critical Information Infrastructure (the Cybersecurity Code). 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 (No. 26 of 2012) (PDPA) and the Computer Misuse Act (Chapter 50A) (CMA).

Under the PDPA, organisations are required to make reasonable security arrangements to protect personal data in its possession or under its control to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (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 CMA, existing sector-specific frameworks have been put in place by the relevant regulators that address cybersecurity issues. For example, the telecommunications and media regulator, the Info-communications Media Development Authority (IMDA), has issued the Telecommunications Cybersecurity Code of Practice (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 formed using 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 and the MAS Guidelines on Outsourcing, which require financial institutions, among other things, to notify the MAS of breaches of security and confidentiality of financial institutions' 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 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 Common Criteria.

1 Section 24 of the PDPA.

2 International Organisation for Standardisation/International Electrotechnical Commission.

3 Internet Engineering Task Force.

Regulatory bodies

Enforcement of the Cybersecurity Act

The regulatory body responsible for enforcing the Cybersecurity Act is the Cybersecurity Agency of Singapore (CSA). The CSA provides dedicated and centralised oversight of national cybersecurity functions to protect essential services. The CSA 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 the Commissioner, who is also the chief executive of the CSA. Assistant commissioners may also be appointed to assist the Commissioner. The CSA also 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.

The relevant powers prescribed to the Commissioner to aid him or her in the enforcement of the Cybersecurity Act include:

- the power to obtain information to ascertain if a computer or computer system fulfils the criteria or the level of cybersecurity of CIIs;[4]
- the power to issue written directions to the CII owner or class of 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]

As far as we are aware, at the time of writing, the CSA had 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, would generally be responsible for investigating and prosecuting cyber crimes under the CMA.

The data protection authority, the Personal Data Protection Commission (PDPC), is responsible for enforcing the PDPA, and may impose on an organisation that fails to comply with the protection obligation a financial penalty of up to S$1 million. The PDPC may also impose on the organisation such directions as it thinks fit in the circumstances to ensure compliance with the protection obligation. We highlight that one of the amendments in the proposed draft Personal Data Protection (Amendment) Bill 2020 is to increase the maximum financial penalty that may be imposed by the PDPC to the higher of 10 per cent of an organisation's annual turnover or S$1 million. As of the time of writing, this change has yet to take effect.

4 Sections 8 and 10 of the Cybersecurity Act.

5 Section 12 of the Cybersecurity Act.

6 For more detail, see sections 19 and 20 of the Cybersecurity Act.

7 Sections 38 and 39 of the Cybersecurity Act.

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

Relevant obligations for companies 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 or 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. Such audits are to 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 such obligations may be provided for under the Cybersecurity Code. The CSA will also be periodically introducing supplementary references to help owners of CII 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 process. The Security-by-Design is an approach that addresses the cyber protection considerations throughout a system's life cycle and it is one of the key components of the Cybersecurity Code.

With regard to the protection of personal data, unless an exception applies, 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.

To assist organisations with compliance with the protection obligation, and other data protection obligations in the PDPA, 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

8 Section 10 of the Cybersecurity Act.
9 Sections 11 and 12 of the Cybersecurity Act.
10 Section 13 of the Cybersecurity Act.
11 Section 14 of the Cybersecurity Act.
12 Section 15 of the Cybersecurity Act.
13 Section 15 of the Cybersecurity Act.
14 Section 16 of the Cybersecurity Act.

consider adopting. Other relevant guides include the PDPC's Guide to Securing Data in the Electronic Medium (revised 20 January 2017) as well as the PDPC's Guide to Data Protection by Design for ICT Systems (issued 31 May 2019).

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.

The Cybersecurity Act's CII protection framework applies to any CII located wholly or partly in Singapore.[15] In addition, as mentioned above, a computer or computer system located wholly or partly in Singapore may be designated as a CII.[16] 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 IT systems and data from cyber threats'.

The data protection provisions under the PDPA apply to all organisations that are not public agencies or acting on behalf of public agencies, whether or not formed or recognised under the laws of Singapore or resident or having 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 has extraterritorial effect. The CMA provides that the provisions of the CMA shall have effect, in relation to any person, whatever his 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, he or she 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 or create a significant risk of seriously diminishing public confidence in the provision of an essential service include publication to the public of the medical records of patients of a hospital in Singapore, or providing access to the public to the account numbers of customers of a bank in Singapore.

15 Section 3 of the Cybersecurity Act.
16 Section 7 of the Cybersecurity Act.
17 Section 2(1) of the PDPA.
18 Section 11(1)–(2) of the CMA.
19 Section 11(3) of the CMA.

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 under section 36 of the Cybersecurity Act.[21]

Moreover, a director's failure to adequately manage an organisation's cybersecurity arrangements may amount to a breach of his directors' duties, for example, under section 157 of the Companies Act (Chapter 50), which requires a director to use reasonable diligence in the discharge of the duties of his or her 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;
- 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 after becoming aware of the occurrence and, within 14 days after 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
- what remedial measures have been taken.[23]

20 Section 36 of the Cybersecurity Act.
21 Section 37 of the Cybersecurity Act.
22 Section 14 of the CMA.
23 Regulation 5 of the CII Regulations.

The prescribed cybersecurity incidents mentioned above are:

- the unauthorised hacking of CII;
- 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
- 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 mitigating 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

There is currently no mandatory requirement or procedure under the PDPA for organisations to report data breaches to the PDPC.

However, the requirement for organisations to report data breaches to the PDPC was proposed in the draft Personal Data Protection (Amendment) Bill 2020, which was published 14 May 2020. Specifically, under this amendment, organisations will be required to notify the PDPC of a data breach that is likely to result in significant harm or impact to the individuals to whom the data relates (eg, if it affects any prescribed class of personal data), or is of a significant scale (ie, if 500 or more individuals are affected). The organisation must make the notification within three calendar days of assessing that a breach is notifiable to the PDPC. As at the time of writing, the Personal Data Protection (Amendment) Bill 2020 has yet to be introduced in Parliament and the changes have yet to take effect.

In terms of the present best practices in a data breach scenario, the PDPC's Guide to Managing Data Breaches 2.0 recommends that organisations carry out their assessment of the data breach within 30 days from when they first became aware of a potential data breach. The details of the data breach and post-breach responses should be recorded in an incident record log to allow follow-up investigations or reviews.

If upon assessment, the organisation is of the view that the breach is likely to result in significant harm or impact to the individual to whom the information relates, or is of a significant scale (involving personal data of 500 or more individuals), the organisation should notify the PDPC of the breach as soon as practicable, no later within 72 hours. Organisations may also wish to notify the affected individuals as soon as practicable where significant harm or impact to the individual is likely.

As best practices, the notification to the PDPC should include the following information:

- extent of the data breach;
- type and volume of personal data involved;

24 Regulation 5 of the CII Regulations.

- cause or suspected cause of the breach;
- whether the breach has been rectified;
- measures and processes that the organisation had put in place at the time of the breach;
- information on whether affected individuals of the data breach were notified and, if not, when the organisation intends to do so; and
- contact details of persons the PDPC can contact for further information or clarification.

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.

Further, according to the PDPC's Advisory Guidelines on Enforcement of Data Protection Provisions, the fact that an organisation has voluntarily notified the PDPC of a data breach as soon as it learned of the breach and cooperated with the PDPC in its investigations may be mitigating factors that the PDPC will take into account when calculating, if applicable, the financial penalty to be imposed.

Breaches in the financial sector

With respect to the financial sector, the MAS Notice on Technology Risk Management (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. The TRM Notice also requires financial institutions to submit a root cause and impact analysis report to MAS within 14 days, or such longer period as MAS may allow, from the discovery of the relevant IT incident.

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.[25] This right is only exercisable after the PDPC has made a decision under the PDPA in respect of a breach, and the decision has become final as a result of all avenues of appeal being exhausted.

The Criminal Procedure Code provides that, if a person is convicted of any offence, the court shall, after the conviction, consider whether or not to make an order for the payment by that person of a sum to be fixed by the court by way of compensation to the person injured, in respect of his person, character or property by the offence or offences for which the sentence is passed, and any offence that has been taken into consideration for the purposes of sentencing only.[26] Thus, should an individual be convicted of a cyber crime under the CMA, the court may also order compensation to any other person who has suffered injury as a result of that offence.

25 Section 32 of the PDPA.

26 Section 359 of the Criminal Procedure Code (Cap 68).

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

Updates and trends

Singapore has been increasingly paying more attention to cybersecurity issues in the past year. In July 2019, the second Government Bug Bounty Programme was announced, and was expanded to cover more systems and digital services. Registered and authorised hackers will receive rewards ranging from US$250 to US$10,000, depending on the severity of the discovered vulnerability. Discovered vulnerabilities will then be reported to the relevant organisation for remediation.

In addition, to strengthen Singapore's operational cybersecurity capabilities, the Singapore 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 cyber attacks and development of cybersecurity standards, as well as to collaborate on regional cybersecurity capacity building. Singapore has signed MOUs with Australia, Canada, France, India, the Netherlands, the United Kingdom and the United States. In addition, Singapore has signed a Joint Declaration on Cybersecurity Cooperation with Germany and a memorandum of cooperation on Cybersecurity with Japan.

In addition, on 17 May 2019, the CSA and The National Cyber Policy Office (NCPO) of New Zealand signed a formal arrangement to strengthen cybersecurity cooperation. Singapore and New Zealand will undertake cybersecurity cooperation in key areas including regular information exchange on cybersecurity incidents and threats, and sharing of best practices on the protection of critical information infrastructure and cyber ecosystem development. Both countries will also conduct cybersecurity exercises and collaborate on capacity building activities in the region.

On 23 November 2019, Singapore and the Republic of Korea signed an MOU to enhance cooperation and information sharing on cybersecurity. This MOU will facilitate more exchanges and information-sharing across the strategic, policy, and technical domains, including in the areas of protection of critical information infrastructure, the promotion of the cybersecurity ecosystem, as well as human resource development, so as to strengthen the ability of both states to address and tackle the transboundary challenge of cybersecurity.

On 23 March 2020, Singapore renewed its 2017 MOU on cybersecurity cooperation with Australia, to further strengthen and expand cooperation and information sharing. The MOU will promote cooperation in information exchange and sharing; joint cybersecurity exercises; training to develop awareness and skills; sharing of best practices and promoting innovation; regional confidence-building measures; and regional capacity building.

In addition, Singapore has also sought to build strategic partnerships with the industry. On 3 October 2019, CSA and FireEye 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.

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, have not yet come into effect. Given the impact of the covid-19 pandemic (as at the time of writing), it is unclear when the relevant provisions will be brought into effect.

As mentioned above, the PDPC has also published the draft Personal Data Protection (Amendment) Bill 2020, which will, among other things, introduce a mandatory data breach notification regime. Under this, organisations will be required to notify the PDPC and affected individuals of data breaches that are likely to result in significant harm or impact to the individuals to whom the information relates. At the time of writing, the mandatory data breach notification requirement is not yet in effect, though the Personal Data Protection (Amendment) Bill 2020 is expected to be tabled in Parliament and implemented in due course.

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 cyber attack 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 managing director, corporate and finance with Drew & Napier LLC. He heads Drew & Napier's technology, media and telecommunications, and is co-head of the firm's data protection, privacy and cybersecurity practice.

Chong Kin is cited by many publications as a leading lawyer in the fields of telecommunications, media and technology. He is highly regarded by his peers, clients and rivals alike 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 a wide range of 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 Infocomm Development Authority in liberalising the telecom industry and developing the Telecom Competition Code, and the 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. To date, Chong Kin continues to advise clients in cutting-edge ICT, data protection, and cybersecurity matters.

Charis Seow
Drew & Napier LLC

Charis' key practice areas are data protection, technology, media and telecommunications (TMT), and compliance and regulatory matters.

Charis assists clients on Singapore data protection law compliance, including reviewing contractual agreements and policies, developing and implementing compliance programmes, conducting training sessions, as well as advising on enforcement issues relating to security, access, monitoring and data breaches. In addition to her experience advising private-sector clients, Charis was seconded to the Personal Data Protection Commission (PDPC) for two years and assisted on wide-ranging issues relating to legislative development, policy and enforcement.

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 Info-communications Media Development Authority (IMDA)/Personal Data Protection Commission (PDPC) in setting up and 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, privacy and cybersecurity matters. These matters run the full gamut, including the implementation of group-wide data protection compliance programmes, the localisation of global data privacy policies, data protection training programmes, the requirements of Singapore's Cybersecurity Act 2018, developing a data breach management plan, dealing with data breaches and cybersecurity incidents (whether involving hacking, malware or accidental disclosure), data breach reporting obligations under Singapore law, 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

Charis Seow
charis.seow@drewnapier.com

The GDR Insight Handbook 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.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

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

an LBR business

ISBN 978-1-83862-266-4