
CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

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

Singapore: Law and Practice

Lim Chong Kin, David N Alfred,
Albert Pichlmaier and Goh Boon Yeow
Drew & Napier LLC



SINGAPORE



Law and Practice

Contributed by:

Lim Chong Kin, David N Alfred, Albert Pichlmaier and Goh Boon Yeow
Drew & Napier LLC

Contents

1. General Overview of Laws and Regulators p.5

- 1.1 Cybersecurity Regulation Strategy p.5
- 1.2 Cybersecurity Laws p.6
- 1.3 Cybersecurity Regulators p.8

2. Critical Infrastructure Cybersecurity p.10

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.10
- 2.2 Critical Infrastructure Cybersecurity Requirements p.10
- 2.3 Incident Response and Notification Obligations p.12
- 2.4 State Responsibilities and Obligations p.12

3. Financial Sector Operational Resilience Regulation p.12

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.12
- 3.2 ICT Service Provider Contractual Requirements p.13
- 3.3 Key Operational Resilience Obligations p.14
- 3.4 Operational Resilience Enforcement p.14
- 3.5 International Data Transfers p.16
- 3.6 Threat-Led Penetration Testing p.17

4. Cyber-Resilience p.19

- 4.1 Cyber-Resilience Legislation p.19
- 4.2 Key Obligations Under Legislation p.19

5. Security Certification for ICT Products, Services and Processes p.19

- 5.1 Key Cybersecurity Certification Legislation p.19

6. Cybersecurity in Other Regulations p.20

- 6.1 Cybersecurity and Data Protection p.20
- 6.2 Cybersecurity and AI p.21
- 6.3 Cybersecurity in the Healthcare Sector p.22

Drew & Napier LLC established a dedicated Data Protection, Privacy and Cybersecurity Practice to leverage its unrivalled experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional companies, multinationals, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries. At the forefront of

data protection law in Singapore since 2013, the Data Protection, Privacy and Cybersecurity Practice Group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection and Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external Data Protection Officer services.

Authors



Lim Chong Kin is the managing director of Drew & Napier's Corporate and Finance department, heads the Telecommunications, Media and Technology Practice and

co-heads the Data Protection, Privacy and Cybersecurity Practice. With his strong background in competition, data protection and technology laws, Chong Kin offers clients expert commercial advice. He has been an external legal and regulatory adviser for the Personal Data Protection Commission of Singapore since it was established in 2013. He also played a key role advising Singapore's Infocom regulator, the Info-communications Media Development Authority. Chong Kin is highly regarded by his peers, clients and rivals for his expertise, and is consistently recommended as a leading lawyer by major international legal publications.



David N Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy and Cybersecurity Practice Group. He is concurrently co-head and

programme director of the Drew Data Protection and Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 25 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet. He has substantial experience advising on data protection and cybersecurity compliance, regulatory enforcement, data breaches and international aspects of data protection. Prior to joining the firm, David was the first Chief Counsel of Singapore's data protection authority, the Personal Data Protection Commission.



Albert Pichlmaier is a senior cybersecurity and privacy engineer with Drew & Napier LLC and concurrently a senior learning technology designer of the Drew Data Protection and

Cybersecurity Academy. Albert is an IT professional with over 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation to AI and blockchain development, as well as IT security product certifications. Albert holds a degree in computer science and CISSP and CDPSE certifications. Prior to joining the firm, Albert worked for over ten years in the public sector in Singapore, most recently for Singapore's data protection authority.



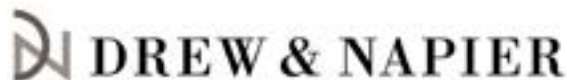
Goh Boon Yeow is an associate director of Drew & Napier's corporate and finance department. Boon Yeow's main areas of practice are technology, media and telecommunications

(TMT), broadcasting, cybersecurity, data protection and privacy, and employment law. He regularly advises leading global and local telecommunications and broadcasting companies on corporate, commercial, licensing and regulatory issues. Prior to joining Drew & Napier, Boon Yeow served in the public service as a legal counsel on an overseas scholarship, where he advised on a broad range of contentious and non-contentious issues.

Drew & Napier LLC

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: chongkin.lim@drewnapier.com
Web: www.drewnapier.com



1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

The first iteration of the Singapore Cybersecurity Strategy was published by the Cyber Security Agency of Singapore (CSA). It outlined measures to build resilient infrastructure, and create a safer cyberspace for Singapore, among other objectives. The strategy was revised in 2021 to take a more proactive stance to addressing the evolving cyber threat landscape. The Singapore Cybersecurity Strategy 2021 extends the previous strategy by recognising the emergence of disruptive technologies like edge computing and quantum technologies, alongside increasingly sophisticated threat actors exploiting pervasive connectivity.

Developed in consultation with multiple stakeholders, including industry, and local and overseas academia, the 2021 strategy aims to proactively defend Singapore's cyberspace, simplify cybersecurity for users, and advance international cybersecurity norms. The 2021 strategy also emphasises the importance of a strong cybersecurity workforce and ecosystem as key enablers of Singapore's cybersecurity. Key components of the 2021 strategy include the following.

Three Strategic Pillars

- **Building resilient infrastructure:** beyond expanding the CSA's regulatory remit under the Cybersecurity Act 2018, the CSA also encourages enterprises and organisations to adopt a risk management mindset (as opposed to a compliance mindset) and invest in their digital infrastructure.
- **Enabling a safer cyberspace:** the government will take the lead in securing digital infrastructure and support the development of a

healthy digital environment. In particular, the government will make it easier for everyone to secure their devices and use secure applications.

- **Enhancing international cyber co-operation:** the government will advance the development and implementation of voluntary, non-binding norms, which sit alongside international law. The government will also advocate the development and adoption of technical and interoperable standards and step up operational co-operation with international partners.

Two Foundational Enablers

- **Developing a vibrant cybersecurity ecosystem:** the government will galvanise the cybersecurity industry and academia to develop advanced capabilities, build world-class products and services, and grow Singapore's cybersecurity market.
- **Growing a robust cyber talent pipeline:** the government will work closely with schools to educate students in cybersecurity and nurture budding cybersecurity enthusiasts and partner with industry and institutes of higher learning to develop skills and competency frameworks for cybersecurity professionals.

The Singapore Cybersecurity Strategy 2021 underscores Singapore's commitment to a multi-faceted approach to cybersecurity, recognising the shared responsibility of all stakeholders in safeguarding the nation's digital interests.

In terms of cybersecurity regulation, the dedicated cybersecurity law, the Cybersecurity Act 2018 (see further details at **1.2 Cybersecurity Laws**), had three objectives when it was first promulgated:

- first, to strengthen the protection of Singapore's critical information infrastructure (CII) against cyber-attacks;
- secondly, to authorise the CSA to lead in the prevention and response to cybersecurity threats and incidents;
- thirdly, to establish a licensing framework to regulate cybersecurity service providers.

In 2024, the government saw the need to update the Act to keep pace with changes in technology, business models and the cyber threat landscape. In so doing, the amendments will allow CSA to extend their regulatory oversight to important systems and entities not previously covered under the Cybersecurity Act 2018, adopting a risk-based approach to regulating entities for cybersecurity.

1.2 Cybersecurity Laws

Cybersecurity in Singapore is broadly regulated by a set of overlapping pieces of legislation which address the issues of national cybersecurity, cybercrimes, and personal data protection and management. In addition, certain sectoral regulators are empowered to directly address cybersecurity issues in their respective sectors through the issuance of regulatory codes, guidelines, notices and instruments.

Cybersecurity Act 2018 (Cybersecurity Act)

The Cybersecurity Act is the dedicated cybersecurity law which sets out the overarching framework for the oversight of national cybersecurity issues in Singapore, including the designation of computer systems as CII in essential sectors and co-ordinating the national response to cybersecurity incidents, amongst other things.

The Cybersecurity Act requires owners of CII to notify the Commissioner of Cybersecurity in the event of the occurrence of certain cybersecu-

riety incidents related to their CII. In this regard, a cybersecurity incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.

Since 2022, the Cybersecurity Act provides for the licensing of certain cybersecurity service providers (CSPs). At present, this includes CSPs that provide penetration-testing and managed security operations centre monitoring services.

To keep up with the evolving cybersecurity threats and nature of businesses, the Cybersecurity (Amendment) Bill was passed in Singapore Parliament on 7 May 2024 to expand the CSA's oversight to new entities beyond CII owners. The four new categories (please see **2.2 Critical Infrastructure Cybersecurity Requirements** for further details) of entities are:

- essential service providers who use CII owned by a third party;
- major foundational digital infrastructure (FDI) service providers;
- entities of special cybersecurity interest; and
- owners of systems of temporary cybersecurity concern.

Importantly, the amendments have extended the definition of CIIs to include any computer or computer system, whether they are physical or virtual, located wholly or partly in Singapore which may be designated as CII. Such designation may arise if the Commissioner is satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore. At

the time of writing, the amendments have yet to come into force.

Computer Misuse Act 1993 (CMA)

The CMA sets out the enforcement and penalty framework against perpetrators of cyber-related offences, such as the unauthorised access to and modification of computer material, unauthorised use or interception of a computer service, unauthorised obstruction of use of a computer and unauthorised disclosure of a password or access code. The CMA empowers the police and other government authorities to investigate and prosecute perpetrators of cybercrimes.

Personal Data Protection Act 2012 (PDPA)

The PDPA applies to all private sector organisations that collect, use, disclose or otherwise process personal data (both electronic and non-electronic data). Personal data is defined as data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

As part of complying with the PDPA, organisations are required to make reasonable security arrangements (which may include technical and cybersecurity measures) to protect personal data in their possession or under their control to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks; or (ii) the loss of any storage device or medium on which personal data is stored.

The PDPA also includes notification requirements in the event of a data breach, that is (i) the occurrence of unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (ii) loss of any storage device or medium on which personal data is stored where unauthorised access, col-

lection, use, disclosure, copying, modification or disposal of personal data is likely to occur.

The Do Not Call (DNC) provisions under the PDPA regulate the sending of certain marketing messages to Singapore telephone numbers. These provisions are intended to give individuals more control over the type of marketing messages they may receive by allowing individuals to register their telephone numbers with the DNC Registry and imposing obligations on organisations in respect of sending marketing messages. This thereby reduces the number of unsolicited messages received by individuals and the risk of being exposed to cybersecurity attacks.

The DNC provisions impose restrictions on whether an organisation may send specified messages (as defined in Section 37 of the PDPA) to a Singapore telephone number. Organisations must check that the Singapore telephone number it intends to send a specified message to is not registered with the DNC Registry before sending the specified message, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in evidential form. Further, Section 48B prohibits organisations from sending any message to a recipient's telephone number where that telephone number was obtained by a dictionary attack or through address-harvesting software. Section 48A of the PDPA defines dictionary attack as the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations. On the other hand, address-harvesting software refers to software that is designed for searching the internet for telephone numbers and harvesting those numbers. Thus, although the DNC provisions primarily target marketing messages, they serve a secondary

role of reducing the ways in which malicious actors may conduct cyber-attacks.

Spam Control Act 2007 (SCA)

The SCA provides for the control of spam and for matters connected with spam in Singapore. The SCA generally regulates the sending of electronic messages with a Singapore link and contains specific obligations relating to senders of unsolicited commercial electronic messages in bulk. Such obligations include the use of the label “<ADV>” to mark unsolicited commercial electronic messages and to offer an unsubscribe option to recipients. The SCA also prohibits the sending of an electronic message to an electronic address obtained through the use of a dictionary attack or address-harvesting software. The SCA is a civil penalty regime where non-compliance with these requirements may result in civil actions against the spammer.

Public Sector (Governance) Act 2018 (PSGA)

Aside from the confidentiality and secrecy provisions found across various legislation, data protection and management in the public sector is also governed under the PSGA. The PSGA, which aims to strengthen public sector data governance, imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or re-identify anonymised data. Specific data security policies are further set out in the Government Instruction Manual on IT Management.

Other Sectoral Frameworks

Two notable examples are in the telecommunications and banking and finance sectors.

First, in the area of telecommunications, the telecoms and media regulator, the Info-communications Media Development Authority (IMDA),

has published a Telecommunications Cybersecurity Code of Practice to enhance cybersecurity preparedness of designated telecommunication licensees such as internet service providers in Singapore. This Telecommunications Cybersecurity Code of Practice, which was formulated in line with international standards and best practices including the ISO/IEC 27011 and IETF Best Current Practices, sets out requirements on security incident management and other controls to help licensees prevent, protect, detect and respond to cybersecurity threats.

Secondly, the Singapore financial regulatory authority, the Monetary Authority of Singapore (MAS), has issued its Technology Risk Management (TRM) Guidelines (the “TRM Guidelines”), which set out risk management principles and best practices to guide financial institutions (FIs) in establishing sound and robust technology risk governance and oversight, as well as in maintaining IT and cyber-resilience. In conjunction with this, the MAS has also issued legally binding Notices on TRM and Cyber Hygiene which give effect to some of the requirements in the TRM Guidelines. Please also see **3.1 Scope of Financial Sector Operation Resilience Regulation** for further details.

1.3 Cybersecurity Regulators

Cyber Security Agency of Singapore

The regulatory authority responsible for the administration and enforcement of the Cybersecurity Act is the CSA. The CSA is part of the Prime Minister’s Office and is managed by the Ministry of Digital Development and Information (MDDI), and led by the Commissioner of Cybersecurity. The Minister for Digital Development and Information (as the Minister-in-charge of Smart Nation and Cybersecurity) may appoint Assistant Commissioners from sectoral regulators who understand the unique context and

complexity of their respective sectors to advise and assist the Commissioner on the co-ordination of cybersecurity efforts.

Under the Cybersecurity Act, the Commissioner's functions and duties include, but are not limited to:

- advising the Singapore government or any other public authority on cybersecurity matters;
- monitoring and responding to cybersecurity threats, whether such cybersecurity threats occur in or outside Singapore;
- identifying and designating computer systems as CII in essential sectors, and regulating owners of CII;
- establishing cybersecurity codes of practice and standards of performance for implementation by owners of CII;
- developing and promoting the cybersecurity services industry in Singapore; and
- licensing and establishing standards in relation to CSPs.

In general, the Cybersecurity Act (as it currently stands) applies to any computer or computer system located wholly or partly in Singapore which may be designated as CII. When the upcoming amendments to the Cybersecurity Act take effect, such CII can also involve any computer or computer system, whether they be physical or virtual. The Commissioner may confer such a designation when they are satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore.

The Cybersecurity Services Regulation Office was set up within the CSA in 2022 to administer the licensing framework of CSPs under the Cybersecurity Act, responding to the industry's queries and feedback, and sharing of resources on licensable cybersecurity services.

Currently, the Singapore government has gazetted a list of 11 sectors in which there may be essential services (ie, services which are essential to national security, defence, foreign relations, the economy, public health, public safety or the public order of Singapore). The 11 sectors include: energy; info-communications; media; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; and services relating to the functioning of the government.

The Commissioner has broad powers to investigate and prevent cybersecurity threats or incidents, including making requests for information to be provided or, in serious cases, direct remedial measures to be taken by any person (including those who are not owners of CII).

Personal Data Protection Commission

The Personal Data Protection Commission (PDPC) is Singapore's data protection authority. The PDPC, which is under the purview of the MDDI, was established in January 2013 and tasked with enforcing and administering the PDPA. With effect from 1 October 2016, the PDPC was merged into the then newly formed IMDA and IMDA was designated as the PDPC. The PDPC is led by the Commissioner for Personal Data Protection.

The PDPA broadly applies to private sector organisations, whether or not formed or recognised under the laws of Singapore or resident or having an office or a place of business in Singa-

pore. As such, foreign businesses that carry out activities involving personal data in Singapore may be subject to the data protection provisions under the PDPA. In terms of notable exclusions, the PDPA does not apply to individuals acting in a personal or domestic capacity, employees acting in the course of their employment with an organisation, and public agencies.

The PDPA confers powers on the PDPC to enforce the PDPA, which include powers relating to:

- alternative dispute resolution (eg, mediation);
- reviews of data subjects' access and correction requests;
- investigations to ensure compliance with the PDPA (including the DNC provisions); and
- undertakings.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Please refer to **1.2 Cybersecurity Laws** and **1.3 Cybersecurity Regulators** for further details on when a CII may fall under the scope of the Cybersecurity Act.

2.2 Critical Infrastructure Cybersecurity Requirements

Generally, owners of CII are required to comply with a set of general duties, such as:

- to comply with notices issued by the Commissioner to provide information on the technical architecture of the CII;
- to comply with codes of practice, standards of performance or written directions in relation to the CII;

- to notify the Commissioner of any change in ownership of the CII;
- to notify the Commissioner of any prescribed cybersecurity incidents (please refer to **2.3 Incident Response and Notification Obligations**);
- to conduct regular audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance;
- to conduct regular risk assessments of the CII as required by the Commissioner; and
- to participate in cybersecurity exercises as required by the Commissioner.

The Cybersecurity Code of Practice for Critical Information Infrastructure (the "CII Cybersecurity Code") requires owners of CII to put in place security baseline configuration standards for all operating systems, applications and network devices of a piece of CII that is commensurate with the cybersecurity risk profile of that CII. The security baseline configuration standards address the following security principles:

- least access privilege and separation of duties;
- enforcement of password complexities and policies;
- removal of unused accounts;
- removal of unnecessary services and applications (eg, removal of compilers and vendor support applications);
- closure of unused network ports;
- protection against malware; and
- timely update of software and security patches that are approved by system vendors.

The CII Cybersecurity Code sets out the following protection requirements that owners of CII need to put in place.

- Access control – CII owners must implement authentication techniques for access into the CII, maintain logs of all access into a CII and of all attempts to access the CII, and review these logs for anomalous activities on a regular basis.
- System hardening – CII owners must establish security baseline configuration standards for the CII.
- Remote connection – CII owners must ensure that all remote connections to the CII have effective cybersecurity measures to prevent and detect unauthorised access.
- Removable storage media – CII owners shall ensure that strict control is exercised over the connection of removable storage media and portable computing devices to a CII.
- Vulnerability assessment and penetration testing – CII owners shall conduct a vulnerability assessment of their CII to identify security and control weaknesses within 12 months from when the CII is designated under the Cybersecurity Act, and at least once every 12 months thereafter for CII that are IT systems; each vulnerability assessment should include (i) a host security assessment, (ii) a network security assessment, and (iii) an architecture security review.

Following the passing of the Cybersecurity (Amendment) Bill, the upcoming Cybersecurity Act will cover four new classes of entities.

- Designated providers of essential services that do not own the CII used for the continuous delivery of the essential services they are responsible for (third-party-owned CII): the providers of such essential services are required to obtain legally binding commitments from the third-party to provide the necessary information or adhere to prescribed standards relating to cybersecurity, etc. The Commissioner may order such providers to cease using the third-party-owned CII if they do not obtain the legally binding commitments.
- Owners of computers or computer systems designated as systems of temporary cybersecurity concern: for example, the temporary systems used to support the distribution of critical vaccines during a pandemic could fall under this category.
- Designated entities of special cybersecurity interest: if the function of such designated entities perform is disrupted, or if the sensitive information contained in their computer systems is disclosed, there will be a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore.
- Designated providers of major foundational digital infrastructure services: these services promote the availability, latency, throughput or security of digital services, and relate to cloud computing services and data facility services.

The upcoming amendments to the Cybersecurity Act impose obligations on these new entities that are similar to those already in force relating to CIIs, such as:

- providing the Commissioner with information;
- complying with any codes of practice, standards of performance or written directions that may be issued or approved by the Commissioner; and
- notifying the Commissioner of any prescribed cybersecurity incident – the exact scope of incident reporting and the applicable cybersecurity codes of practice/standards/guidelines applicable to these new entities have not been published at the time of writing.

2.3 Incident Response and Notification Obligations

Under the Cybersecurity (Critical Information Infrastructure) Regulations 2018, cybersecurity incidents that must be reported to the Commissioner include:

- any unauthorised hacking of the CII or the interconnected computer or computer system to gain unauthorised access to or control of the CII or interconnected computer or computer system;
- any installation or execution of unauthorised software, or computer code, of a malicious nature on the CII or the interconnected computer or computer system;
- any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the CII or the interconnected computer or computer system, and an authorised user of the CII or the interconnected computer or computer system, as the case may be; and
- any denial-of-service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the CII or the interconnected computer or computer system.

2.4 State Responsibilities and Obligations

The Cybersecurity Act sets out a number of duties and functions of the Commissioner of Cybersecurity in relation to the identification and response to cyber threats.

Under Section 5 of the Cybersecurity Act, the Commissioner of Cybersecurity has a duty, among others:

- to monitor cybersecurity threats in or outside of Singapore;
- to advise the government or any other public authority on the national needs and policies in respect of cybersecurity matters generally; and
- to respond to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services of Singapore, whether such cybersecurity incidents occur in or outside Singapore.

Additionally, the Singapore Computer Emergency Response Team (SingCERT), which is part of the CSA, routinely issues cybersecurity and cyber hygiene advisories and alerts. SingCERT also works with the sectoral regulators to issue relevant alerts and advisories to industry players and to inform companies and affected individuals on cybersecurity threats and incidents.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

Please refer to **1.2 Cybersecurity Laws** for a summary of the sectoral cybersecurity laws applicable to the banking and finance sector.

In the banking and finance sector, the MAS has issued a set of legally binding Notices on TRM and Cyber Hygiene which apply to FIs (eg, banks, insurers, capital markets services licence holders, operators, and settlement institutions of designated payment systems). These Notices impose obligations on FIs to enhance information security and mitigate the growing risks of cyberthreats.

The TRM Notices include requirements to:

- put in place a framework and process to identify critical systems;
- make reasonable efforts to maintain a high availability of critical systems;
- establish a recovery time objective for each critical system;
- notify the MAS of a system malfunction or IT security incident;
- submit a root cause and impact analysis report to the MAS of the relevant incident within 14 days; and
- implement IT controls to protect customer information from unauthorised access or disclosure.

The Notices on Cyber Hygiene include requirements to:

- secure administrative accounts;
- apply security patching;
- establish baseline security standards;
- deploy network perimeter defences;
- implement anti-malware measures; and
- strengthen multi-factor authentication.

3.2 ICT Service Provider Contractual Requirements

Under the TRM Guidelines, MAS sets out a number of principles and best practices to in relation to third-party service providers, which include:

- ensuring service providers have the requisite level of competence and skills to perform IT functions and manage technology risks;
- conducting IT security awareness training programmes for service providers who have access to FIs' information assets;
- identifying threats and vulnerabilities applicable to information assets that are maintained or supported by service providers;

- assessing service providers' disaster recovery capability and ensuring that disaster recovery arrangements are established, tested and verified to meet FIs' business needs;
- ensuring service providers are accorded the same level of protection and subject to the same security standards in data security as FIs;
- involving service providers in scenario-based cyber exercises to validate FIs' response and recovery, as well as communication plans against cyber threats; and
- reporting of phishing attempts to service providers.

More generally, ICT service providers may fall under the upcoming category of designated providers of major foundational digital infrastructure services under the Cybersecurity Act. "Foundational digital infrastructure services" are services that promote the availability, latency, throughput or security of digital services, and have been specified in the Third Schedule to the upcoming Cybersecurity Act. This will include a "cloud computing service" and a "data centre facility service", as set out below.

- A "cloud computing service" is defined as a service, delivered from a computer or computer system in Singapore or outside Singapore, that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources.
- A "data centre facility service" is defined as any service which relies on a computer or computer system in Singapore to facilitate data storage, processing and transmission by another person through the centralised accommodation, interconnection and operation of one or more computers or computer

systems, encompassed within a facility in Singapore dedicated to that purpose.

Under the upcoming Cybersecurity Act, designated providers of major FDI services will be subject to obligations such as providing the Commissioner with information, reporting prescribed cybersecurity incidents, and complying with codes of practices and directions that may be issued or approved by the Commissioner.

On 1 March 2024, the legislature announced that the inter-agency Taskforce on the Resilience and Security of Digital Infrastructure and Services is studying the introduction of a Digital Infrastructure Act to further enhance the resilience and security of key digital infrastructure and services in Singapore. At the time of writing, there is no publicly available information on the obligations imposed on digital infrastructure providers under the upcoming Digital Infrastructure Act.

3.3 Key Operational Resilience Obligations

The key obligations relating to digital operation resilience in the financial sector can be derived from Part 8 of the TRM Guidelines relating to IT resilience. The best practices that FIs should aim to comply with include:

- establishing system availability commensurate with its business needs;
- establishing system recoverability aligned to its business resumption and system recovery priorities;
- regularly testing their disaster recovery plans to validate their effectiveness and meet the defined recovery objectives;
- establishing a system and data backup strategy so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted; and

- conducting a Threat and Vulnerability Risk Assessment for their data centres to identify potential vulnerabilities, and the protection that should be established to safeguard the data centres against physical and environmental threats.

In terms of incident reporting obligations, FIs should establish cyber-incident response and management plans to swiftly isolate and neutralise cyber threats and to securely resume affected services. The plan should describe communication, co-ordination and response procedures to address plausible cyber threat scenarios. Each FI should seek to understand their exposure to technology risks and place a robust risk management framework to ensure cyber resilience.

FIs may also be designated as CII under the Cybersecurity Act. For more information on the designation of CII and the obligations imposed on CII under the Cybersecurity Act, please refer to [1.2 Cybersecurity Laws](#), [1.3 Cybersecurity Regulators](#) and [2.2 Critical Infrastructure Cybersecurity Requirements](#).

3.4 Operational Resilience Enforcement

There are no specific obligations relating to operation resilience in relation to critical ICT service providers. However, critical ICT service providers in the financial sector can take guidance from Part 8 of the TRM Guidelines (please refer to [3.3 Key Operational Resilience Obligations](#) for further details).

Generally, under Section 29(1) of the Financial Services and Markets Act, MAS has the power to issue directions or make regulations concerning any FI or class of FIs as the MAS considers necessary for:

- the management of technology risks, including cybersecurity risks;
- the safe and sound use of technology to deliver financial services; and
- the safe and sound use of technology to protect data.

In terms of enforcement action, an FI that fails to comply with a direction issued to it under Section 29(1) or contravenes any regulation mentioned in that subsection shall be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD1 million and, in the case of a continuing offence, to a further fine of SGD100,000 for every day or part of a day during which the offence continues after conviction.

The maximum penalty of SGD1 million is commensurate with the most serious types of breaches that can be committed by FIs. This quantum was derived after considering comparable existing penalty regimes of other Singapore government agencies and the need to signal the importance of TRM.

Additionally, under the current Cybersecurity Act, the Commissioner has broad powers under Sections 19 and 20 to investigate and prevent cybersecurity incidents and “serious” cybersecurity incidents respectively. These include powers to require persons to attend interviews, require the production of relevant information (such as physical or electronic records, or documents that are in the possession of that person), carry out questioning, give directions to carry out remedial measures or cease activities, require assistance with investigations, enter premises, access and inspect computer systems, among others.

It is an offence for any person to fail to co-operate with the CSA without reasonable excuse and

such persons shall be liable on conviction to be punished in accordance with the fines, terms of imprisonment or both, as set out in the relevant statutory provisions.

Under the upcoming Section 18K(1) of the upcoming Cybersecurity Act, the Commissioner may require major FDI service providers to furnish information. If the major FDI service provider fails to, without reasonable excuse, furnish the required cybersecurity-related information within the specified period or continues providing the designated FDI service despite the non-compliance, they shall be guilty of an offence. They shall be liable for a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the service provider’s business in Singapore.

The upcoming Section 18L(1) also empowers the Commissioner to issue written instructions to major FDI service providers which may relate to the action to be taken by the provider in relation to a cybersecurity threat, compliance with any prescribed technical standards relating to cybersecurity, among others. Any major FDI service provider who fails to comply with such a written direction and continues to provide FDI infrastructure service after the deadline for compliance will be liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person’s business in Singapore.

Further, under the upcoming Section 18M (1), major FDI service providers must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the major FDI, where the incident results in a disruption or degradation to the continuous delivery of the foundational digital infrastructure service or the major FDI service provider’s business operations in Singapore. Any major FDI service provider

who, without reasonable excuse, fails to comply with this obligation shall be guilty of an offence and liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person's business in Singapore.

As the provisions relating to the obligations for major FDI service providers have yet to come into force, there are no enforcement decisions against major FDI service providers for the failure to comply with the Cybersecurity Act.

3.5 International Data Transfers

There are no specific obligations imposed by MAS in relation to financial institutions carrying out international data transfers. However, generally, organisations transferring personal data overseas must comply with Section 26 of the PDPA. Under Section 26, organisations need to ensure that the personal data transferred overseas is accorded a standard of protection that is comparable to the protection under the PDPA.

Under the Personal Data Protection Regulations 2021 (the "PDP Regulations"), the transferring organisation must take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

"Legally enforceable obligations" include any of the following obligations which are imposed on the recipient of the personal data under:

- any law;
- any contract requiring the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA

and specify the countries and territories to which the personal data may be transferred under the contract;

- any binding corporate rules that require every recipient of the transferred personal data that is related to the transferring organisation to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA; and which specifies:
 - (a) the recipients of the transferred personal data to which the binding corporate rules apply;
 - (b) the countries and territories to which the personal data may be transferred under the binding corporate rules; and
 - (c) the rights and obligations provided by the binding corporate rules; and
- any other legally binding instrument, including the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors System or the APEC Cross Border Privacy Rules System, which are recognised under the PDP Regulations as one of the modes of transferring data overseas.

The transferring party is required to specify the countries and territories to which the personal data may be transferred under the contract if the party relies on imposing contractual obligations on the recipient for the data transfer.

A transferring party has taken the appropriate steps to ensure that the recipient is bound by legally enforceable obligations to provide the personal data transferred a standard of protection that is comparable to that under the PDPA if:

- the data subject whose personal data is to be transferred gives their consent to the transfer of their personal data, after being provided with a reasonable summary in writing of the

extent to which the personal data transferred to those countries and territories will be protected to a standard comparable to the protection under the PDPA; or

- the transfer is necessary for the performance of a contract between the organisation and the data subject, or to do anything at the data subject's request with a view to their entering a contract with the organisation.

As good practice, however, organisations are encouraged to rely on the above circumstances only if they are unable to rely on legally enforceable obligations or specified certifications.

In respect of international data transfers between regulatory authorities in the financial sector, the MAS is a signatory to the Administrative Arrangement (AA) for the Transfer of Personal Data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory Authorities.

The AA sets out the safeguards relating to data transfers between regulatory authorities which include purpose limitation, data quality and proportionality, transparency, security and confidentiality, data subject rights, onward transfers and sharing of personal data, data retention periods, and redress. As a signatory, MAS confirms that it adheres to the safeguards outlined in the AA.

More generally, Singapore joined the APEC Cross-Border Privacy Rules System and Privacy Recognition for Processors System in 2019, which are accountability-based and enforceable certifications developed by APEC economies for cross-border transfers of personal data.

In January 2021, the member states of the Association of Southeast Asian Nations (ASEAN) approved the ASEAN Data Management Frame-

work (DMF), and the Model Contractual Clauses for Cross Border Data Flows (MCCs), which are resources and tools for ASEAN businesses to utilise in their data-related business operations. In summary, the DMF provides a common data protection framework for businesses on good data management practices and best practices, while the MCCs are a set of template contractual terms and conditions that may be included in the binding legal agreements between parties transferring personal data to each other across borders.

In May 2023, the Joint Guide to ASEAN MCCs and EU Standard Contractual Clauses (SCCs) was launched (the "Joint Guide"). The Joint Guide provides a comparison between ASEAN MCCs and SCCs for organisations looking to transfer or receive consumer data from overseas partners. Companies already familiar with the ASEAN MCCs can use the Joint Guide as a reference in their contractual negotiations on data transfers with their EU business partners.

3.6 Threat-Led Penetration Testing Critical Information Infrastructure

Under the CII Cybersecurity Code, owners of CII are required to conduct regular penetration testing on CII to identify security vulnerabilities that could be exploited by a cyber threat actor. This allows organisations to determine exploitable vulnerabilities in their systems and address them.

Owners of CII are required to conduct a penetration test on the CII:

- at least once every 12 months, for CII which is an information technology system; and
- at least once every 24 months, for CII which is an operational technology system.

Owners of CII must also conduct penetration tests on relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning any new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.

It is the responsibility of CII owners to ensure that third-party penetration testing service providers and their penetration testers possess industry-recognised accreditations and certifications respectively, for example CREST or equivalent accreditations and certifications.

Relatedly, owners of CII are also required to establish a red teaming or purple teaming attack simulation plan, and conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months to test and validate the effectiveness of its cybersecurity measures against prevalent cybersecurity threats.

Cybersecurity Service Provider Licences

The Cybersecurity Services Regulation Office (CSRO) was set up to administer the licensing framework for CSPs under the Cybersecurity Act. It aims to address three main considerations:

- provide greater assurance of security and safety to consumers;
- improve the standards and standing of CSPs; and
- address the information asymmetry between consumers and CSPs.

All providers of a managed security operations centre monitoring services and penetration testing services as defined in the Cybersecurity Act to the Singapore market must apply to the CSRO for a cybersecurity service provider's

licence, regardless of whether they are companies or individuals or third-party CSPs that provide these services in support of other CSPs.

IoT Devices

On 3 March 2020, the MDDI (then Ministry of Communication and Information) introduced the Cybersecurity Labelling Scheme (CLS) as part of Singapore's Safer Cyberspace Masterplan 2020. The CLS was formally launched on 7 October 2020, initially as a voluntary scheme for Wi-Fi routers and smart home hubs, and was subsequently expanded to include all smart home devices.

The CLS provides different cybersecurity rating levels for registered IoT devices and other smart devices to help consumers easily assess the level of security offered and make informed choices in purchasing a device. A Level 1 certification indicates that the product meets basic security requirements such as ensuring unique default passwords and providing software updates, whilst a Level 4 certification indicates that the product has undergone structured penetration tests by approved third-party test labs and fulfilled the requirements of all lower levels (ie, Levels 1, 2 and 3).

In 2024, the CSA updated Singapore's Operational Technology Cybersecurity Masterplan. The updated Masterplan now includes operators of operational technologies that support physical control functions such as IoT and industrial IoT devices, as such devices have become new attack surfaces for threat actors to exploit. The key initiatives under the Masterplan include:

- enhancing the operational technology cybersecurity talent pipeline;
- enhancing information sharing and reporting;

- uplifting operational technology cybersecurity resilience beyond CII; and
- promoting secure-by-development principles.

ICT Systems Containing Personal Data

As Section 24 of the PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks, penetration testing may be helpful in determining whether the organisation is in compliance with the PDPA. Furthermore, the PDPC's Guide to Data Protection Practices for ICT Systems and Guide to Data Protection by Design for ICT Systems generally recommend the conduct of penetration testing to ensure data protection measures operate as intended and to detect any vulnerabilities.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

The Singapore Cybersecurity Strategy 2021 emphasises enhancing response capabilities for the state, organisations and individuals rather than an emphasis on expanding legislation relating to cyber-resilience (please refer to **1.1 Cybersecurity Regulation Strategy** for more details).

As such, apart from the Cybersecurity Act, and the patchwork of other cybersecurity and sectoral legislation mentioned in **1.2 Cybersecurity Laws**, the legislative status of cyber-resilience in Singapore remains relatively sparse compared to other jurisdictions such as the European Union which has the dedicated Cyber Resilience Act.

4.2 Key Obligations Under Legislation

Please refer to **1.2 Cybersecurity Laws**, **2.2 Critical Infrastructure Security Requirements**, **3.2 ICT Service Provider Contractual Requirements**, **3.3 Key Operational Resilience Obligations** and **4.1 Cyber-Resilience Legislation**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

While there is no prescribed cybersecurity certification legislation in Singapore, the CSA offers, administers and supports the use of certification schemes to provide assurance to customers that the product has been objectively assessed from a cybersecurity standpoint.

The CSA Cybersecurity Certification Centre operates three schemes which cover ICT product security in general. For example, besides the CLS, the Singapore Common Criteria Scheme (SCCS) provides a cost-effective regime to evaluate and certify the security of IT products in Singapore against the Common Criteria (CC) standards (ie, ISO/IEC 15408 series). CC is a common set of standards initially developed through a collaboration among national security and standards organisations in Canada, France, Germany, the Netherlands, the UK and the USA. Under the Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security (also known as Common Criteria Recognition Arrangement (CCRA)), which forms the basis of international recognition of CC certifications, Singapore's SCCS is recognised as a Certificate Authorising Scheme. The CC harmonises the evaluation (which ranges from document review to deep penetration testing) of IT products by defining a common set of security func-

tions which product developers use, to establish the security requirements of their IT products in a standardised language.

The PDPC and the IMDA jointly developed the Data Protection Trustmark (DPTM) Certification to help organisations demonstrate compliance with the PDPA. The DPTM Certification serves as a visible indicator that organisations have adopted sound data protection practices, strengthening trust between customers, business partners and regulators to increase business competitiveness. The DPTM Certification aligns its requirements with the PDPA and also incorporates elements of international benchmarks and data protection best practices.

Singapore has also joined the APEC Cross-Border Privacy Rules System and Privacy Recognition for Processors System in 2019 (see [3.5 International Data Transfers](#)).

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

In terms of broad focus and application, the Cybersecurity Act addresses national cybersecurity issues and protects computers and computer systems in Singapore by imposing obligations on owners of CII. In contrast, the PDPA seeks to protect consumers and individuals by imposing obligations on private sector organisations that collect, use, disclose or otherwise process personal data.

General Requirements Under the PDPA

In the context of personal data protection, organisations are required to, amongst other things, put in place data protection policies and practices to ensure and demonstrate compli-

ance with their obligations under the PDPA. Specifically, these requirements include:

- appointing a data protection officer to oversee compliance with the PDPA;
- developing and implementing data protection policies, practices and procedures (which include technical security arrangements) to ensure proper processing of personal data;
- providing adequate training to staff that handle and process personal data; and
- conducting a data protection impact assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual (where applicable).

Protection Obligation

Additionally, under the protection obligation (Section 24 of the PDPA), an organisation is required to make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

Data Breach Notification

With effect from 1 February 2021, a mandatory data breach notification regime has been introduced into the PDPA.

A “data breach” in relation to personal data is defined in the PDPA to mean:

- the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection,

use, disclosure, copying, modification, or disposal of the personal data is likely to occur.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or control has occurred, it must conduct an assessment of whether the data breach is a “notifiable data breach” in a reasonable and expeditious manner.

A data breach is a “notifiable data breach” if the data breach (i) results in, or is likely to result in, significant harm to an affected individual; or (ii) is, or is likely to be, on a significant scale (ie, affecting at least 500 persons).

According to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (the “Data Breach Regulations”), a data breach is deemed to result in significant harm to an individual if the data breach relates to the following:

- the individual’s full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual as set out in the schedule to the Data Breach Regulations.
- all of the following personal data relating to an individual’s account with an organisation:
 - (a) the individual’s account identifier, such as an account name or number; or
 - (b) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to, or use of, the individual’s account.

Notification to the PDPC

Upon assessing that the data breach is a “notifiable data breach”, the organisation must notify the PDPC in the prescribed form and manner as soon as practicable but no later than three

calendar days after assessment. This notification to the PDPC must contain all the relevant information of the data breach to the best of the knowledge and belief of the organisation.

Notification to Affected Individuals

Upon notifying the PDPC, the organisation must also notify each individual affected by the data breach, unless an exception applies. An organisation does not need to notify affected individuals in two circumstances:

- if, on or after assessing that the data breach is a “notifiable data breach”, the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or
- if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data breach will result in significant harm to the affected individual.

Notification to the Primary Organisation

Where a data intermediary processing personal data on behalf of another organisation has reason to believe a data breach has occurred, it must, without undue delay, notify the primary organisation.

6.2 Cybersecurity and AI

Computers or computer systems which support AI solutions may be designated as a CII under the Cybersecurity Act if they are necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore, and the computer or computer system is located wholly or partly in Singapore. For more details on which entities may be designated as CII and the obligations that a CII will have to

comply with, please refer to **1.2 Cybersecurity Laws**, **1.3 Cybersecurity Regulators** and **2.2 Critical Infrastructure Cybersecurity Requirements**.

While there are no express cybersecurity obligations relating to AI in Singapore at the time of writing, a number of voluntary frameworks and guidelines have been published relating to the development and use of AI.

The second edition of the Model AI Framework was published by the PDPC on 21 January 2020. The framework sets out the common definitions and principles relating to the responsible use of AI generally, making practical recommendations that organisations can readily adopt to deploy AI responsibly.

On 30 May 2024, the Model AI Governance Framework for Generative AI, which sets out a systematic and balanced approach to address generative AI concerns while facilitating innovation, was published by IMDA and AI Verify Foundation. In particular, the framework recommends that generative AI developers adapt the “security-by-design” concept, which involves designing security into every phase of the systems development life cycle of an AI, to fit the specific characteristics of generative AI. New security safeguards which the framework recommends be developed include input filters, which are moderation tools designed to detect unsafe prompts, and digital forensics tools, which can be used to investigate digital data to reconstruct cybersecurity incidents stemming from a generative AI model.

The framework also makes recommendations with regard to incident reporting. As part of an overall proactive security approach, AI software product owners should adopt vulnerability

reporting before incidents happen. After incidents happen, organisations need internal processes to report the incident for timely notification and remediation. Depending on the impact of the incident and how extensively AI was involved, organisations should consider notifying both the public as well as the government.

On 15 October 2024, the CSA published the Guidelines and Companion Guide on Securing AI Systems. The Guidelines address potential security risks through the AI lifecycle, and help to protect AI systems against traditional cybersecurity risks such as supply chain attacks, and novel risks such as adversarial machine learning. On the other hand, the companion guide offers practical security control measures that system owners may consider in implementing these guidelines. Key recommendations include taking a lifecycle approach to consider security risks and beginning with a risk assessment.

Lastly, the Engaging with Artificial Intelligence guide, which was published on 25 January 2024 by the Australian Signals Directorate’s Australian Cyber Security Centre in conjunction with the CSA and 13 other international agencies, also provides organisations with guidance on how to use AI systems securely. The guide summarises some important threats related to AI systems and prompts organisations to consider steps they can take to engage with AI while managing risk. The document provides cybersecurity mitigations to assist organisations that use self-hosted and/or third-party hosted AI systems.

6.3 Cybersecurity in the Healthcare Sector

While there are no specific cybersecurity obligations pertaining to the healthcare sector, the healthcare sector has been gazetted as one of 11 sectors providing essential services. As such,

designated owners of CII within the healthcare sector would be subject to the same requirements as laid out in **2.2 Critical Infrastructure Cybersecurity Requirements**.

Beyond CII, there are a number of security requirements relating to devices in the medical field. Depending on the type of medical device, the relevant regulators may include the Health Sciences Authority (HSA), the National Environment Agency and the IMDA. Where applicable, healthcare providers must also comply with the National Telemedicine Guidelines, which include data protection and security requirements. Insofar as a medical device is used by an organisation to collect personal data (eg, device test results are uploaded onto a server owned by the organisation), the organisation must comply with the protection obligation under the PDPA (as described in **6.1 Cybersecurity and Data Protection** above).

On 4 December 2023, the Cyber and Data Security Guidelines for Healthcare Providers (Healthcare Guidelines) was published. The Healthcare Guidelines provide guidance on the cyber and data security measures to be put in place for the proper storage, access, use and sharing of health information to improve the security posture amongst healthcare providers. Healthcare providers looking to better understand and meet the Healthcare Guidelines can also refer to the Cyber and Data Security Guidebook for healthcare providers for explanations and references to resources from the CSA and PDPC. While not mandatory, the requirements within the Healthcare Guidelines will eventually be imposed as regulatory requirements under the upcoming Health Information Act, which has yet to come into force at the time of writing.

In October 2024, the Cybersecurity Labelling Scheme for Medical Devices (CLSMD), which was jointly developed by the CSA, Ministry of Health, HSA and Synapse, was launched. Under this voluntary scheme, medical devices are rated according to four levels of cybersecurity provisions, with each level indicating a progressively higher standard of security. The label aims to improve security awareness by making the cybersecurity provisions of medical devices more transparent to healthcare users, thereby empowering them to make more informed purchasing decisions.

The CLSMD applies to medical devices as described in the First Schedule of the Health Products Act 2007 that have any of the following characteristics:

- handle personal identifiable information and clinical data, and can collect, store, process, or transfer such data; and
- connect to other devices, systems, and services, and can communicate using wired and/or wireless communication protocols through a network of connections.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com