ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Thailand

Saroj Jongsaritwang

R&T Asia (Thailand) Limited

Sui Lin Teoh

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

The main laws and regulations relating to computer crimes in Thailand are the Computer Crime Act 2007 ("**CCA**") and the Thai Penal Code.

Hacking (i.e. unauthorised access)

Yes. Section 5 of the CCA provides that whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for that person's use would be liable to imprisonment not exceeding six months or to a fine not exceeding THB 10,000, or both.

Section 7 of the CCA provides that whoever illegally accesses computer data that has specific security measures which are not intended for that person's use would be liable to imprisonment not exceeding two years or to a fine not exceeding THB 40,000, or both.

Denial-of-service attacks

Yes. Section 10 of the CCA provides that whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference to a computer system of another person so that it is not capable of functioning normally would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Phishing

Yes. Section 14(1) of the CCA provides that whoever dishonestly or deceitfully inputs into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the public (but not constituting a crime of defamation) under the Penal Code, would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Section 9 of the CCA provides that whoever illegally acts in a manner that damages, impairs, deletes, alters or makes additions to, either in whole or in part, computer data of another person would be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

No. However, the Thai Court has the power to forfeit any property used or in possession for use in the commission of an offence by any person.

Identity theft or identity fraud (e.g. in connection with access devices)

No. There is no specific offence in relation to identity theft or identity fraud. However, identity theft/fraud would be considered as the act of causing damage to the computer data of another person under Section 9 of the CCA mentioned above. In addition, whoever inputs into a publicly accessible computer system computer data that will appear as an image of another person and the image has been created, edited, appended or adapted by electronic means or whatsoever means, and in doing so is likely to impair the reputation of such other person or exposes such other person to hatred or contempt, would be liable to imprisonment not exceeding three years and a fine not exceeding THB 200,000, or both (Section 16 of the CCA).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

This is not applicable in our jurisdiction.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. Section 6 of the CCA provides that if a person who has knowledge of the security measures to access a computer system specifically created by another person illegally discloses such security measures in a manner that is likely to cause damage to another person, such person shall be liable to imprisonment not exceeding one year or to a fine not exceeding THB 20,000, or both.

Section 8 of the CCA provides that a person who illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilise would be liable to imprisonment not exceeding three years or to a fine not exceeding THB 60,000, or both.

Failure by an organisation to implement cybersecurity measures

Yes. Section 15 of the CCA provides that any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 of the CCA with regards to a computer system in his control would be liable to the same penalty as provided in Section 14 of the CCA.

Section 14 of the CCA provides that whoever commits the following acts shall be liable to imprisonment not exceeding five years or to a fine not exceeding THB 100,000, or both:

(1) dishonestly or deceitfully inputting into a computer system computer data which is distorted or forged, either in whole or in part, or computer data which is false, in such a manner likely to cause injury to the public but not constituting a crime of defamation under the Criminal Code;

(2) inputting into a computer system computer data which is false, in such a manner likely to cause damage to the maintenance of national security, public safety, national economic security, or public infrastructure serving national public interest, or to cause panic amongst the public;

(3) inputting into a computer system computer data which constitutes a crime concerning the security of Thailand or a crime concerning terrorism under the Penal Code;

(4) inputting into a computer system computer data with vulgar characteristics when such computer data is capable of being accessed by the general public; and

(5) publishing or forwarding computer data with the knowledge that it is the computer data under points (1) to (4).

If the acts under (1) to (5) above are not committed against the public but are committed against a particular person, the criminal or the person who publishes or forwards the aforesaid computer data would be liable to imprisonment not exceeding three years or to a fine not exceeding THB 60,000, or both (and the offences are compoundable).

1.2 Do any of the above-mentioned offences have extraterritorial application?

If an offence specified in the CCA is committed outside Thailand and (i) the offender is a Thai national and there is a request for punishment by the government of the country where the offence has occurred or by the injured person, or (ii) the offender is a non-Thai national and the Thai Government or a Thai person is an injured person and there is a request for punishment by the injured person, the offender would be subject to the provisions of the CCA.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes. There is an exception which applies only to service providers. In principle, any service provider who cooperates, consents to or acquiesces in the commission of an offence under Section 14 of the CCA with regards to a computer system within his control would be subject to the same penalty as that which is imposed upon a person who commits the offence under Section 14 of the CCA. However, in the case that the service provider is able to prove it has complied with the Ministerial Notification setting out procedures for the notification and suppression of the dissemination of such data and the removal of such data from the computer system, it would be exempt from the penalty (Section 15 of the CCA).

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Yes. Section 269/4 of the Criminal Code provides that whoever uses or acquires for use an electromagnetic record/electronic card which is forged or altered in accordance with Section 269/1 shall be liable to imprisonment of between one and 10 years or to a fine of THB 20,000 to THB 200,000, or both. For example, three men were accused of conspiring to hack and forge electronic card information in the systems of a telecommunications operator to raise the cards' top-up value to THB 105,000,000 and then selling them for THB 12,000,000. They were found guilty of selling forged electronic cards and were imprisoned.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

- The CCA.
- The Electronic Transactions Act 2001.
- The Royal Decree prescribing Criteria and Procedures for Electronic Transactions of the Government Sector 2006.
- The Notifications issued by the Electronic Transactions Commission ("**ETC**").
- The Royal Decree on Security Procedures for Electronic Transaction 2010.
- The Special Case Investigation Act 2004.
- The Telecommunication Business Act 2011.
- Payment Systems Act 2018.
- The National Council for Peace and Order Announcements.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. The ETC's List of Sectors/Organisations that are deemed as Critical Infrastructure and Required to Comply with Strict Security Techniques 2016 impose a list of critical infrastructure organisations which are required to have additional security standards (strict security techniques) in accordance with the Notification of the ETC on Information Security Standards and in accordance with Security Techniques 2012, such as having a teleworking policy, automatic equipment identification, a clean-desk policy, a clear-screen policy and setting up time limits on connections with networks regarded as high risk.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Commercial banks, e-payment service providers and telecommunications service providers are required by Applicable Laws to take measures to monitor, detect, prevent and mitigate Incidents as per the requirements set out under Applicable Laws (e.g. Bank of Thailand's Notifications and the Notifications of the National Broadcasting and Telecommunications Commission ("**NBTC**"). Please find more details in our answers to question 3.2 below.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

No, there are no conflict of laws issues.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under the Payment Systems Act, e-payment service providers are required to notify Bank of Thailand ("**BOT**") of an occurrence of any problem or failure to provide e-payment service as soon as possible. E-payment service providers have the obligation to notify BOT of all the problems and failures in relation to their services regardless of whether or not such problem/failure is caused by the occurrence of an Incident. Moreover, e-payment service providers are required to notify BOT within 24 hours if their services are temporarily suspended due to any special circumstances (which may or may not involve an Incident).

With respect to securities companies under the Securities and Exchange Act 1992 ("**SEA**"), securities companies are required to notify, either by verbal or electronic means, the Securities and Exchange Commission ("**SEC**") without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement. The notice is required to specify the date and time of the Incident, the type of Incident, the details of the Incident and the effects from the Incident. On the following business day after such acknowledgment, a written report must be submitted to the SEC, which must further specify details of how the Incident is being resolved and the progress made in doing so.

There are no exemptions applicable to e-payment service providers or securities companies in terms of reporting requirements.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Yes. When an Incident occurs, the organisation is entitled to file a report to the police and that report is then handed to the inquiry official to investigate the alleged conduct and file charges against a suspect (if considered appropriate).

There are no legal provisions prohibiting or restricting organisations from notifying foreign authorities or private sector organisations.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

The securities companies are required to notify an affected customer or other affected persons without delay upon the acknowledgment of a system disruption, unauthorised access to a system or an Incident that results in damage to the security company's reputation, such as website defacement. There are no specific requirements on the information to be included in the notice given to the affected individuals.

For other sectors, there is no legal requirement to notify Incidents or potential Incidents to any affected individuals.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No. The responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

(a) BOT is the regulator of financial institutions and other non-financial institutions as specified by BOT. It is the body responsible for supervising, examining and analysing the performance and risk management systems of e-payment services.

(b) The SEC is the regulator of companies listed on the Stock Exchange of Thailand and is responsible for supervising the standard operating procedures of securities companies, including IT supervision procedures.

(c) A police officer has the authority to initiate an investigation or proceedings relating to a criminal offence, including CCA offences.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

(a) With respect to securities companies under the SEA, the penalty for not complying with the notice requirements under questions 2.5 and 2.7 is a fine not exceeding THB 300,000 and a further fine not exceeding THB 10,000 for every day during which the violation continues. The director, manager or any person responsible for the operation of such securities company shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding THB 200,000, or both, unless it can be proven that such person has no involvement with the commission of the offence by such securities company.

(b) With respect to e-payment service providers under the supervision of BOT, the penalty for not complying with the notice requirement under question 2.5 is a fine not exceeding THB 1,000,000 or THB 2,000,000 depending on the type of e-payment service providers.

(c) With respect to telecommunications business licensees, they are required to comply with the licensing conditions prescribed in their particular licence, which may include cybersecurity measures. In such case, if a licensee fails to comply with the prescribed licensing conditions, the National Broadcasting and Telecommunications Commission shall have the power to order the licensee to: refrain from carrying out the violating act(s); carry out rectification and improvement; or perform actions correctly or appropriately within a specified period of time. If the licensee fails to comply with the order, the licensee shall be liable to a fine of not less than THB 20,000 per day and in case the licensee still omits to perform the actions correctly, or where there is serious damage to the public interest, the Commission shall have the power to suspend or revoke the licence.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

So far, we have found no non-compliance cases taken by the relevant regulators which have been announced to the public.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. State agencies have obligations pertaining to specific information security measures, such as the requirement for policies and practices on personal information protection in electronic transactions, IT security practices and policies (which must include provisions relating to access control, user access management, user responsibilities, network control, operating system access control and other provisions as specified by the Office of the Electronic Transactions Commission ("**OETC**")). On the other hand, private sector organisations have fewer legal requirements.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Yes.

(a) Financial services sector: organisations which operate e-payment services are regulated under the relevant BOT notifications. Principally, e-payment service providers are required to have a contingency plan or a backup system for the purposes of continuity of the service and a safety policy or measures for the information system, which must at least meet the standards prescribed in the BOT notifications. Moreover, e-payment service providers are required to keep customer data confidential throughout and after the use of its services, with certain exceptions. The OETC may also prescribe mandatory practices required to be observed by the e-payment service provider.

(b) Telecommunications sector: the telecommunications sector is administrated by the National Broadcasting and Telecommunications Commission ("**NBTC**"). The NBTC has issued notifications setting out rules and procedures for the management of information technology, and procedures for protecting personal information, rights of privacy and freedom in communication through telecommunications' means. Moreover, the NBTC has the power to prescribe specific provisions concerning cybersecurity to each licensed telecommunications operator.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There are none in our jurisdiction.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Securities companies are required to conduct cyber risk assessments and vulnerability assessments at least once a year. If a securities company assigns a third party to manage its IT system, the securities company is required to have an Incident response policy. There is no requirement for the appointment of a CISO for securities companies.

These requirements do not apply to private companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Securities companies are required to submit an annual report which includes its IT management and occurrence of Incidents to the SEC. E-payment service providers are also required to prepare information and details as to the provision of services and make the same available for inspection by BOT. BOT has the power to instruct an e-payment service provider to provide any information in relation to its services, including information on the occurrence of Incidents.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

The CCA imposes a legal requirement on service providers (e.g. a website service provider) to keep and maintain certain computer data (e.g. IP address, logs) depending upon the characteristics of the service provider. Examples are the requirement to keep relevant computer traffic data in order to be able to identify the user from the beginning of the use of the service and the log showing the use by such user, and store it for not less than 90 days after the end of the service period. The competent official is empowered on a case-by-case basis to order a service provider to maintain such computer traffic data for a period not exceeding two years.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Issues relating to Incidents are governed by the Civil and Commercial Code ("**CCC**") under the section relating to a "wrongful act" (i.e. Section 420 of the CCC). A wrongful act is similar to a tort. Under this provision of law, if any Incident, whether wilfully or negligently, unlawfully damages or injures another person's life, body, health, liberty, property or any right, the party in breach is said to have committed a wrongful act and is bound to pay compensation for damages suffered. The general guidance from the Thailand Supreme Court's decisions is that the injured party is entitled to claim actual damage suffered, with the burden of proof being on the claimant.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

In 2016, the accused was arrested in connection with the attacks that caused some government websites to be blocked and non-public files to be leaked. The legal status of the accused is not yet available to the public.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

Yes. Please see the response to question 5.1 above.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in our jurisdiction.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are no regulatory limitations.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

No, there are not any specific requirements under Applicable Law.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are not any Applicable Laws that may prohibit or limit the reporting of the above.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

For the benefit of an investigation, if there is reasonable cause to believe that there is a perpetration of an offence under the CCA, or there is a request by the inquiry official, the competent official is empowered to acquire evidence to prove an offence and to identify the accused, for example, by: (i) issuing an inquiry letter to any person related to the commission of an offence to give statements, forward written explanations or any other documents, data or evidence in a comprehensible form; (ii) requiring computer traffic data related to communications from a service user via a computer system or from other relevant persons; (iii) instructing a service provider to (a) deliver user-related data that is required to be retained under the CCA requirements or that is in the service provider's possession or control to the competent official, or (b) keep the data for later; or (iv) seizing or attaching a computer system for the purposes of obtaining details of the offence and the person who committed the offence.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Yes. As mentioned in question 8.1 above, the competent official has the authority to access a computer system, computer data, computer traffic data or a computer data storage device and to decrypt the computer data of any person, provided that the competent official has obtained a court order to do so.

Saroj Jongsaritwang
R&T Asia (Thailand) Limited
973 President Tower
12th Floor Units 12A – 12F
Ploenchit Road Lumpini Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: saroj.jongsaritwang@rajahtann.com
URL: th.rajahtannasia.com

Saroj is a Partner in the Corporate & Commercial Practice of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann LLP. Saroj graduated with a Bachelor of Laws from Thammasat University in 1999, and is a licensed Thai lawyer.

Prior to joining Rajah & Tann, Saroj was a legal counsel (AVP) at a leading Thai consumer finance business, and before that he was in private practice at a local Thai law firm. Saroj has several years' experience in advising on corporate, commercial and consumer finance matters (including personal loans, credit cards and insurance) and agreements relating to the consumer finance business. He regularly advises on employment and TMT matters and is recommended in *The Legal 500* for 2015, 2016, 2017 and 2018 for TMT and Employment, and in *Chambers Asia Pacific* (2017, 2018) in TMT and Banking.

Sui Lin Teoh
R&T Asia (Thailand) Limited
973 President Tower
12th Floor Units 12A – 12F
Ploenchit Road Lumpini Pathumwan
Bangkok 10330
Thailand

Tel: +66 2 656 1991
Email: sui.lin.teoh@rajahtann.com
URL: th.rajahtannasia.com

Sui Lin is the Deputy Managing Partner of R&T Asia (Thailand) Limited, the Bangkok office of Rajah & Tann LLP. Sui Lin graduated with a Bachelor of Laws from the University of London, and is qualified as a solicitor in England & Wales. Before joining Rajah & Tann, Sui Lin was Of Counsel in the dispute resolution group of an international law firm in Thailand. Prior to that, she was a partner in a leading local law firm. She has more than 24 years of experience in Thailand, advising on general corporate and commercial matters, including advising clients in the telecommunications sector and e-commerce businesses on setting up operations in Thailand, and on the handling and use of data under Thai law. She also regularly advises on employment matters and is recommended in *The Legal 500* 2018/19 in this area. Sui Lin is fluent in spoken Thai.

RAJAH & TANN
Thailand

Based in Bangkok, the team in R&T Asia (Thailand) Limited has an impressive base of international, regional and local clients.

We have many years of experience in advising on a range of Thai law matters, including representing clients in civil, criminal or administrative proceedings, international and domestic arbitration, government investigations and compliance proceedings, structuring foreign direct investment and mergers and acquisitions involving private or listed companies, and general corporate commercial matters for foreign investors in Thailand.

The team has particular expertise in representing clients in highly regulated industries, such as telecoms, tobacco, food and beverage, insurance and manufacturing, and can provide full support in large-scale litigation, transactions and investigations.

The team comprises a majority of Thai nationals who are qualified to advise on Thai law. Our Thai lawyers are fluent in Thai and English and are fully conversant with the practical application of the law within Thailand's business and cultural landscapes.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com