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:

Korea

Seung Soo Choi

JIPYONG LLC

Seungmin Jasmine Jung

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:

Hacking (i.e. unauthorised access)

Under the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Network Act"), it is prohibited for anyone to infiltrate another's information communication network ("ICN") without authorised access or beyond the scope of authorised access. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million. In a recent court decision, the defendant who infiltrated another's ICN in order to distribute malware was subject to imprisonment of 18 months.

Under the Electronic Financial Transactions Act (the "EFTA"), any unauthorised access of electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Denial-of-service attacks

Under the Network Act, it is prohibited to cause disruption of an ICN by intentionally disturbing network operations with large volumes of signal/data or superfluous requests. Any violation shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

Also, under the EFTA, any attacks on electronic financial systems using programs such as a computer virus, logic bomb or email bomb with the intention of destroying data on, or disrupting the operation of, electronic financial systems shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Phishing

For the regulation of phishing crimes, the Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (the "Special Act on Financial Fraud") has been enacted. Under the Special Act on Financial Fraud, anyone found guilty of phishing crimes shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

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

Under the Network Act, it is prohibited for anyone to transmit or distribute malware that can damage, destroy, alter, falsify or disrupt the operation of ICN systems, data or programs, without a justifiable cause. Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

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

The use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools) is prohibited under the Network Act. Any violation shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 70 million.

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

Under the Personal Information Protection Act ("PIPA"), anyone who commits, or aids and abets, the illegitimate acquisition of personal information, being processed by another party for subsequent provision to a third party for commercial gain or for illegitimate purposes, shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

Also, under the Network Act, it is prohibited for anyone to collect another person's information, or induce the provision of another person's information, through the ICN by deceptive means. Any violation shall be subject to imprisonment of not more than three years or a penalty of not more than KRW 30 million.

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

Any theft of the company's critical information by a company's employee or former employee shall be punished under the Criminal Act as a breach of fiduciary duty or under the Act on Prevention of Unfair Competition and Protection of Trade Secrets as divulging of trade secrets. Any such theft shall be subject to imprisonment of not more than 10 years or a penalty of not less than KRW 30 million under the Criminal Act and imprisonment of not more than five years or a penalty of not more than KRW 50 million under the Act on Prevention of Unfair Competition and Protection of Trade Secrets. Any infringement of the employer's copyright shall be subject to imprisonment of not more than five years or a penalty of not more than KRW 50 million.

There have been several cases where a former employer was criminally prosecuted for taking, without permission, material assets or intellectual property rights of the employer upon termination of employment.

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

Under the Network Act, it is prohibited for anyone to damage another person's information processed, stored or transmitted through the

ICN or to infringe, exploit or disclose another person's confidential information.

Under the EFTA, anyone who falsifies or alters access means shall be subject to imprisonment of not more than seven years or a penalty of not more than KRW 50 million.

Failure by an organisation to implement cybersecurity measures

Under PIPA and its Enforcement Decree, personal information processors have the obligation to implement technical, managerial and physical measures in order to procure security, such as establishing internal control plans and storing access records to ensure personal information is not lost, stolen, leaked, falsified, altered or damaged. In the event personal information is lost, stolen, leaked, falsified, altered or damaged due to a person's failure to implement such measures, such person shall be subject to imprisonment of not more than two years or a penalty of not more than KRW 20 million.

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

As of yet, there are no regulations regarding extraterritorial application of the above offences.

There is, however, a prohibition of the overseas transfer of personal information. Under PIPA, personal information processers are prohibited from entering into contracts regarding the overseas transfer of personal information with terms in violation of PIPA. "Overseas transfer" is a broad concept dealing with the "actual" transfer of personal information and does not only include the provision of personal information to third parties, but also includes (i) the delegation of personal information processing to a third party located outside of Korea, and (ii) the overseas transfer of personal information due to business transfers or mergers.

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?

In relation to criminal prosecution of personal information leakage accidents, the responsible party may be discharged from liability if requisite measures for procuring security have been implemented or if due care has been exercised and supervision has been properly conducted.

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.

Under the Act On The Protection Of Information And Communications Infrastructure (the "PICIA"), it is prohibited to disrupt or paralyse critical ICN infrastructure facilities such as electronic control or managerial systems related to national security, government administration, military defence, policing, finance, telecommunications, transportation and energy. Any violation shall be subject to imprisonment of not more than 10 years or a penalty of not more than KRW 100 million.

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 following are Applicable Laws in Korea: Personal Information Protection Act ("PIPA"); Act On The Protection Of Information And Communications Infrastructure (the "PICIA"); Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (the "Network Act"); Electronic Financial Transactions Act (the "EFTA"); Credit Information Use and Protection Act (the "Credit Information Act"); Act on the Protection, Use, etc. of Location Information; Act On Prevention Of Divulgence And Protection Of Industrial Technology; and Special Act On The Prevention Of Loss Caused By Telecommunications-Based Financial Fraud And Refund For Loss (the "Special Act on Financial Fraud").

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.

Under the PICIA, managerial organisations have the obligation to establish and implement managerial measures, including physical and technical measures (such as prevention, backup, recovery, etc.), to safely protect the critical ICN infrastructure facilities and managerial data.

Under the Network Act, any ICN service provider must take protective measures to procure the security of ICN used in the provision of ICN services and the reliability of information.

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.

Organisations that operate and manage collective ICN facilities ("Collective ICN Facility Operator") for the ICN service of third parties must take the following protection measures (as prescribed under the Enforcement Decree of the Network Act) for the secure operation of ICN facilities:

(i) technical and managerial measures for access control and monitoring of unauthorised access to ICN facilities;

(ii) physical and technical measures for the protection of ICN facilities from natural disasters and threats, such as terrorist attacks, and for procuring the continuous and secure operation of ICN facilities;

(iii) hiring and assignment of personnel for the secure management of ICN facilities;

(iv) establishment and implementation of internal control measures (including emergency plans) for the secure management of ICN facilities; and

(v) establishment and implementation of technical and managerial measures to prevent the dissemination of infiltration Incidents.

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 conflict of laws issues have arisen yet.

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 Network Act, the ICN provider or a Collective ICN Facility Operator must report any "infiltration Incidents" (defined as Incidents due to attacks on the ICN or the related information system through hacking, a computer virus, logic bomb, email bomb, denial of service, high-powered electromagnetic wave, etc.) to the Ministry of Science and ICT or Korea Internet and Security Agency ("KISA") immediately upon the occurrence of such infiltration Incident.

Under PIPA, in the event of any leakage of personal information which concerns 10,000 or more persons, the personal information processor must report such leakage and subsequent measures, without delay, to the Ministry of Interior and Safety or KISA.

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?

Although not obligated, it would be possible for organisations to voluntarily share information related to Incidents with regulatory authorities.

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.

Under PIPA, once a personal information processer becomes aware of any leakage of personal information, it must notify the owner of the leaked personal information, without delay, of the following:

(i) the type of personal information that has been leaked;

(ii) the timing and circumstances of the leakage;

(iii) the actions that the owner of the personal information can take to minimise any damages resulting from the leakage;

(iv) the protective response measures taken by the personal information processor and relief procedures; and

(v) the name and contact of the department to which the owner of the leaked personal information (who has incurred damages) can file a report.

Under the Credit Information Act, in the event of any credit information leakage, the above items must be notified to the owner of such credit information.

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 differ.

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

The Ministry of the Interior and Safety, the Ministry of Science and ICT, the Financial Services Commission, and KISA.

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

If the requirements under Applicable Laws are not complied with, the relevant authorities may impose a monetary fine. For example, a business that fails to provide notice of a credit information leakage Incident shall be subject to a monetary fine of not more than KRW 50 million.

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

Order the submission of relevant materials and inspections, a corrective order, criminal charges, etc.

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.

There are certain variances under Applicable Laws. Under PIPA, the requirements for information security measures to be adopted by personal information processors differ based on the size of the corporation. Moreover, the requirements for protective measures under the Network Act for ICN service providers and under the Credit Information Act for financial institutions are generally stricter than the common 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?

With regards to the financial services sector, the Credit Information Act and the EFTA prescribe specific legal requirements for financial institutions.

With regards to the telecommunications sector, the following companies need to obtain a certification as to whether they satisfy the prescribed technical and physical protective measures for the security and reliability of ICNs:

(i) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose annual revenue or income is not less than KRW 150 billion; or

(ii) companies such as telecommunication providers or companies who provide information through the telecommunication provider's ICN, whose revenue for the preceding fiscal year is not less than KRW 10 billion or whose average volume of daily users for a three-month period is not less than 1 million.

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?

Unless there are special circumstances, the Representative Director or the CPO (or CISO) shall be liable for any breach of the protective measures prescribed under PIPA, the Network Act and the Credit Information Act.

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?

Under the Network Act, ICN service providers with no fewer than 1,000 employees must appoint a CISO at the senior management level to ensure the security of the ICN system and the secure management of data. The CISO is responsible for the following:

(i) the establishment and management/operation of information protection procedures;

(ii) the analysis/evaluation and improvement of any vulnerabilities in information protection;

(iii) the prevention of and response to infiltration Incidents;

(iv) the establishment of preventive measures for information protection and the architecture/implementation of security measures;

(v) the assessment of preventive security measures for information protection;

(vi) the encryption of critical information and assessments of the adequacy of secure servers; and

(vii) the performance of other information protection measures prescribed under Applicable Laws.

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)?

Under the Network Act, in order to analyse the cause of the infiltration Incident, the Minister of Science and ICT can order the ICN provider and the Collective ICN Facility Operator to:

(i) retain relevant material such as records of access to the ICN;

(ii) submit the relevant material; and

(iii) allow physical access to the business site to investigate the cause of the infiltration Incident.

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

The government may enforce measures against ICN service providers or its users to prevent an offshore leakage of material information related to national industry, the economy and science/technology through ICN overseas disclosure.

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.

In the event the owner of personal information incurs damages due to the violation of PIPA by the personal information processor, such owner of personal information can claim damages against the personal information processor. The personal information processor will be liable unless it can prove that there was no wilful misconduct or negligence attributable to it. If the owner of personal information incurs damages arising from the loss, theft, leak, falsification, alteration or damage of personal information caused by the wilful misconduct or gross negligence of the personal information processor, the court may award up to treble damages. Also, the owner of the personal information may seek statutory damages up to KRW 3 million in the event that loss, theft, leak, falsification, alteration or damage of personal information is caused by the wilful misconduct or gross negligence of the personal information processor. In such case, the personal information provider will be liable unless it can prove that there was no wilful misconduct or negligence attributable to it.

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

In 2014, there was a large-scale leakage of personal information from three major credit card companies. The victims of the leakage, as the plaintiffs, brought a case against the credit card companies and the court awarded damages in the amount of KRW 10,000 to each of the plaintiffs for each Incident of leakage.

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

In cases regarding tort liability, the plaintiff has the burden of proof with respect to the tort of the defendant. However, in cases claiming damages for leakage of personal information or credit information,

the defendant has the burden of proof to show that the Incident is not attributable to the defendant. In other words, the burden of proof is reversed.

6 Insurance

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

Under the Credit Information Act, certain financial institutions have the obligation to take measures, such as taking out insurance, joining a cooperative, or setting aside a reserve to procure funds for damages that may arise due to credit information leakage.

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?

The Financial Supervisory Service has set a minimum insurance coverage limit for the liability of financial institutions against credit information leakage. For example, in the case of banks, such limit is KRW 2 billion.

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?

Under the Act On The Promotion Of Workers' Participation And Cooperation, any installation of monitoring facilities require consultation with the Employee and Employer Council. The Employee and Employer Council is a body established within a company for the purpose of promoting the workers' welfare and the advancement of the company through the participation and cooperation of both the employee and employer.

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?

There are no specific requirements under Applicable Laws.

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.

The following authorities have investigatory powers of law enforcement: National Intelligence Service; National Police Agency Cyber Bureau; Forensic Science Investigation Department of the Supreme Prosecutors' Office; Financial Supervisory Service; and KISA.

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?

There are no specific requirements under Applicable Laws.

Seung Soo Choi
JIPYONG LLC
10F, KT&G Seodaemun Tower
60 Chungjeong-ro, Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1759
Fax: +82 2 6200 0820
Email: sschoi@jipyong.com
URL: www.jipyong.com/en

Mr. Seung Soo Choi is a Partner and Head of the IT/IP Practice Group at JIPYONG LLC. Mr. Choi has advised and represented IT companies and start-ups on copyright, patent and IP cases and has also handled a variety of litigations over the last 20 years, covering civil, criminal and commercial cases. With his significant amount of working-level experience, he is recognised as the leading expert in the areas of intellectual property and IT, patents, confidential business information, related to copyrights and trademarks.

Mr. Choi is well-acquainted with laws relating to cultural art and entertainment/media businesses and personal information protection. Mr. Choi actively participates in various academic societies and lectures courses on international entertainment law, motion pictures law, art law, data privacy law, communication law, and media law at Chung-Ang University Law School. Mr. Choi is also a well-recognised mediator in the area of entertainment at the Korean Commercial Arbitration Board.

Mr. Choi is a member of the Korean Bar and received an LL.B. from Seoul National University and the University of Pennsylvania.

Seungmin Jasmine Jung
JIPYONG LLC
10F, KT&G Seodaemun Tower
60 Chungjeong-ro, Seodaemun-gu
Seoul 03740
Korea

Tel: +82 2 6200 1712
Fax: +82 2 6200 0820
Email: smjung@jipyong.com
URL: www.jipyong.com/en

Ms. Seungmin Jasmine Jung is a Senior Foreign Attorney in the Finance Practice Group and IP·IT Practice Group of JIPYONG LLC.

Ms. Jung represents clients in the finance, fintech, energy, real estate and technology sector and has extensive experience in acquisition finance, project finance, structured finance, derivatives, data privacy, private equity fund investments and M&A transactions. She is also considered one of the foremost experts on cloud computing, cryptocurrency, blockchain and cybersecurity.

Prior to joining JIPYONG, Ms. Jung was the Head of Legal at Amazon Web Services Korea, where she specialised in cloud computing and data privacy. Ms. Jung started her legal career as an associate at the NY office of Hughes, Hubbard & Reed and subsequently worked at Shin & Kim and Franklin Templeton Investments in Seoul, Korea.

Currently, Ms. Jung regularly advises clients on cryptocurrency, blockchain and cloud computing while frequently lecturing at conferences, and contributing articles on legal issues surrounding the 4th Industrial Revolution. Ms. Jung also teaches technology law at Yonsei University, her *alma mater*. She is highly regarded by her clients for her transactional expertise and strong negotiation skills.

Ms. Jung is a member of the New York Bar. Ms. Jung has a J.D. from Columbia Law School and a B.A. in political science and international relations from Yonsei University.

JIPYONG JIPYONG LLC

JIPYONG LLC is one of Korea's leading full-service law firms. We pride ourselves on our global reach and outlook, the depth and breadth of our practice groups and the extensive experience of our lawyers. With our network of 12 international offices and desks in China, Russia, Vietnam, Indonesia, Myanmar, Cambodia, Laos and Iran, etc., we provide a one-stop destination for legal and consulting services to our clients. JIPYONG LLC has a strong base of domestic and international clients who rely on us for not only our local market knowledge and expertise but for our innovative, business-minded solutions. In addition to our pursuit of professional excellence and proactively serving the needs of clients, JIPYONG LLC shares an unwavering commitment to high ethical standards, *pro bono* work and community service.

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