ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

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 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Mexico

Begoña Cancino

Oscar Arias

Creel, García-Cuéllar, Aiza y Enríquez, S.C.

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:

There is no definition in Mexican law for the terms "cybercrime" and "cybersecurity"; however, the Federal Criminal Code regulates illegal behaviours committed through electronic means that could be identified as cybercrimes by the use of electronic means for their commission.

Regarding examples of jurisdiction in Mexico, according to Article 16 of the Political Constitution of the United Mexican States ("Mexican Constitution"), no one shall be molested in his person, family, home, papers or possessions (including private information), except by written order of a competent authority, duly grounded in law and fact, which sets forth the legal cause of the proceeding. In this regard, any non-consented access to private information may be sanctioned by law; thus, only a federal judicial authority may authorise any investigation regarding criminal offences.

Hacking (i.e. unauthorised access)

Article 211*bis* of the Federal Criminal Code provides that whoever, without authorisation, modifies, destroys or causes loss of information contained in systems or computer equipment protected by a security mechanism shall be imposed a prison sentence of six months to two years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00. The aforementioned penalty could be duplicated in case the information is used for one's own benefit or to benefit a third party.

Denial-of-service attacks

The Federal Criminal Code does not provide any definition, or similar definition, for this criminal offence.

Phishing

The Federal Criminal Code does not provide any definition for phishing; however, such criminal offence could be considered as fraud. According to Article 386 of the Federal Criminal Code, a person commits fraud when he/she, with the intent of obtaining a financial gain, handles information through deceit, takes advantage of errors, or misleads a person.

In such case, the relevant authority shall impose a prison sentence of three days to 12 years, as well as a fine of approximately MN$2,400.00 to MN$24,012.00, depending on the value in each case.

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

The Federal Criminal Code does not provide any definition for this criminal offence; however, this type of behaviour is similar to hacking. The aforementioned penalties are applicable in this case.

In case the criminal offence is committed against the state, the relevant authority shall impose a prison sentence of one year to four years, as well as a fine of approximately MN$16,000.00 to MN$48,024.00.

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

The Federal Criminal Code provides this criminal offence as "hacking", which is described above.

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

The Credit Institutions Law provides that a person who produces, manufactures, reproduces, copies, prints, sells, trades or alters any credit card, debit card, cheques or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed a prison sentence of three to nine years, by the relevant authority, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00.

In addition, the Federal Criminal Code provides that a person who, with or without authorisation, modifies, destroys or causes loss of information contained in credit institutions' systems or computer equipment protected by a security mechanism shall be imposed a prison sentence of six months to four years, by the relevant authority, as well as a fine of approximately MN$8,004.00 to MN$24,012.00.

Moreover, a person who without authorisation knows or copies information in credit institutions' computer systems or equipment protected by a security mechanism shall be imposed a prison sentence of three months to two years, as well as a fine of approximately MN$4,002.00 to MN$24,012.00.

All the penalties aforementioned could be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

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

As mentioned, the Credit Institutions Law provides that any person who produces, manufactures, reproduces, copies, prints, sells, trades or alters, any credit card, debit card, cheque or, in general, any other payment instrument, including electronic devices, issued by credit institutions, without authorisation of the holder, shall be imposed a prison sentence of three to nine years, as well as a fine of approximately MN$2,401,200.00 to MN$24,012,000.00. The

penalties aforementioned could be duplicated if the criminal offence is committed by any counsellor, official, employee or service provider of any credit institution.

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: espionage; conspiracy; crimes against means of communication; tapping of communications; acts of corruption; extortion; and money laundering could be considered as threats to the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Failure by an organisation to implement cybersecurity measures

Considering the absence of a specific law which regulates cybersecurity in Mexico, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Federal Law on Protection of Personal Data held by Private Parties ("Data Protection Law") provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

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

Yes; however, Mexico has not yet adopted international standards related to cybersecurity.

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, in the following cases:

1) The Federal Law Against Organized Crime provides: (a) that in the investigation of a crime in which it is assumed on good grounds that a member of organised crime is involved, it is possible to tap private communications; and (b) the obligation of concessionaires, authorised entities and any person holding a means or system that could be intercepted, to cooperate with the authorities, prior to a judicial order.
2) The General Law to Prevent and Sanction Kidnapping Crimes provides the possibility to intercept private communications.
3) The National Security Law, in case of an immediate threat to national security, provides that the Mexican Government must request a judicial warrant to intercept private communications for national security purposes.
4) The Federal Telecommunications and Broadcasting Law ("FTBL"), according to Articles 189 and 190, provides that: (i) concessionaires; (ii) authorised entities; and (iii) service providers of applications or contents, are required to: a) allow the corresponding competent authorities to control and tap private communications; and b) provide the support that such authorities request, in terms of the applicable law.

In addition to the federal legislation provided above, there are state laws that allow the interception of individual communications prior to any request from the relevant state authorities (Public Prosecutor of the corresponding state) to a federal judge.

Intervention of private communications is not allowed in: electoral tax; commercial; civil; labour; or administrative matters, or in the case of communications between the arrested and his/her counsel.

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.

As mentioned, the Federal Criminal Code also regulates as a criminal offence the act of sabotage or unlawful interference with: roads, public services, or state services; steel, electric or basic industries; and centres of production or distribution of weapons, ammunition or military equipment, with the aim of disrupting the economic life of the country or affect their ability to defend.

Also, the relevant Code protects means of communication such as telegrams, telephone lines, radio communications, telecommunication networks, as any component of an installation of production of magnetic or electromagnetic energy or its means of transmission.

In addition, the Federal Criminal Code provides that persons who manufacture, import, sell or lease any device or system, or commit any act with the purpose of decoding any encrypted/protected satellite signal without the legitimate authorisation of the licensed distributor, shall be imposed a prison sentence of six months to four years.

On the other hand, the Law on Negotiable Instruments and Credit Operations sanctions diverse actions that affect any kind of financial payment instrument (e.g., credit or service cards) or the information contained on them.

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 Mexican Constitution;
- The FTBL;
- The Data Protection Law, its Regulations, Recommendations, Guidelines and similar regulations on data protection;
- The Federal Law on Transparency and Access to Public Information;
- The General Law on Transparency and Access to Public Information;
- General Standards as the Mexican Official Standard Regarding the Requirements that shall be Observed when Keeping Data Messages;
- The Law on Negotiable Instruments and Credit Operations;
- The Mexican Federal Tax Code;
- The Credit Institutions Law;
- The Sole Circular for Banks;
- The Industrial Property Law;
- The Mexican Copyright Law;
- The Federal Criminal Code;
- The National Security Law;

- The Federal Labour Law;
- The Federal Law for the Federal Police;
- The National Development Plan 2013–2018;
- The National Programme of Public Security 2014–2018; and
- The National Programme of Security 2014–2018.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, how (and according to what timetable) is your jurisdiction expected to implement the Network and Information Systems Directive? Please include details of any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The authors are not aware of any.

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.

As mentioned, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyber threats; however, the Data Privacy Law provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

In addition to the foregoing, there are certain specific mandatory security measures that certain industries must adopt to protect their customers' data. Banking laws and regulations provide that banks must implement certain security measures in electronic banking transactions and require the use of several passwords depending on the amount and nature of the transaction.

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.

The authors are not aware of any.

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.

There is no obligation to report Incidents or potential Incidents to the authorities; however, the General Law on Transparency and Public Information Access provides, in Article 70 Section XLVII, that authorities shall provide access and keep updated, for statistical purposes, the list of requests made to telecommunications concessionaires, service providers or Internet applications related to the interception of private communications, access to the registry of communications, and the real-time geo-location of communication equipment that contain the object, temporary scope and the legal provisions on which the requirement it supports, if that is the case, mentioning if a judicial warrant was granted.

On the other hand, Data Privacy Laws do not provide a penalty for failure to comply with the rules on reporting threats or breaches; nevertheless, the National Institute for Access to Public Information and Data Protection ("INAI") is empowered to evaluate if the cause that originated a data breach was caused by a failure of compliance or negligence.

By the interpretation of the Mexican Constitution, organisations must cooperate with Government Agencies regarding Incidents; however, no law establishes specific requirements to report Incidents or potential Incidents.

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?

Please refer to our answer in question 2.5.

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.

There is no obligation to report any Incidents or potential Incidents; however, Data Protection Law provides that security breaches that materially affect the property or moral rights of data owners will be reported immediately by the data controller to the data owner, so that the latter can take appropriate action to defend its rights.

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 to questions 2.5 to 2.7 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.

The INAI is in charge of: (i) guaranteeing people's right of access to government public information; (ii) protecting the personal data in possession of the federal government and individuals; and (iii) resolving denials of access to information that the dependencies or entities of the federal government have formulated.

The Federal Telecommunications Institute ("IFT") is in charge of regulating telecommunications and broadcasting services.

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

The Applicable Laws are silent in this regard.

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

This is not applicable in our jurisdiction.

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. According to the Data Protection Law, the data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

On the other hand, the Federal Criminal Code and the Law on Negotiable Instruments and Credit Operations provide several sanctions in order to avoid criminal offences regarding cybersecurity.

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. Regarding financial services, the Law on Negotiable Instruments and Credit Operations and the Credit Institutions Law, including the Federal Criminal Code, are applicable in order to avoid cybercrimes.

The FTBL and the Federal Criminal Code are applicable in this matter.

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 no specific laws in Mexico related to cybersecurity responsibilities or liabilities of personnel and directors. Nevertheless, and in accordance with the Data Protection Law, every private party, individual or organisation that processes personal information (data controller), has the obligation to appoint a data person or department (data protection officer) who will be a representative for the organisation in privacy and data protection matters and in charge, within the organisation, of the correct processing of personal data (including verification of security measures), as well as of processing requests from data owners for the exercise of their rights to access, rectification, suppression or rejection.

In relation to information security, data protection officers shall adopt measures to guarantee due processing of personal data, privileging the interests of the data owners and their reasonable expectation of privacy.

The measures that the data protection officer shall adopt, and that may be related to cybersecurity, include the following: (i) issuing policies and programmes, which shall be mandatory within the organisation; (ii) implementing training programmes; (iii) implementing a monitoring and surveillance system and internal or external audits to verify compliance with privacy policies; (iv) assigning resources for the implementation of programmes and policies related to privacy; (v) implementing a risk-detection programme to identify privacy risks when launching new products, services, technologies and business models as well as risk-mitigation strategies; (vi) periodically reviewing security policies and programmes to determine whether amendments are needed; (vii) performing compliance checks; and (viii) implementing personal data-tracking systems to trace which data are collected and where they are stored.

The Data Protection Law does not provide a specific sanction for data protection officers, responsible personnel and directors.

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?

Regarding personal data, all data controllers must designate a data protection officer or department; however, the Applicable Laws are silent in cybersecurity matters.

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)?

The applicable laws are silent in this regard.

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

The applicable laws are silent in this regard.

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.

According to Article 32 of the Federal Criminal Code, organisations and companies are civilly liable for the damages caused to third parties by crimes committed by their partners, managers and directors. The state is similarly liable for the crimes committed by its public officials.

The Federal Civil Code provides a standard of civil liability established in Article 1910, which provides that a party that illegally causes harm to another person shall be obliged to repair the damage, unless he/she proves that the damage was produced as a consequence of the victim's guilt or negligence.

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

The authors are not aware of any.

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

The authors are not aware of any.

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?

The authors are not aware of any.

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?

There are no specific requirements; however, the Data Protection Law provides that a person who is involved with personal data is obligated to establish and maintain physical and technical administrative security measures and in case of any breach, such employee must notify the data protection officer.

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?

The authors are not aware of any.

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 Applicable Laws empower the following authorities to investigate an Incident: (i) the General Attorney Office; (ii) Public Prosecutors; (iii) the INAI; and (iv) the IFT.

Public Prosecutors in Mexico are in charge of investigating cyber activities and to resolve them, a cyber police has been created to follow up on crimes or unlawful activities committed through the Internet. Complaints directed to the cyber police can be submitted via its website, by phone, or through a Twitter or email account; in addition, the Federal Police have created a scientific division called the National Centre For Cyber-Incidents Response, specialised in providing assistance to the victims or claimants of cyber threats and cyber attacks.

In the case of data protection, the INAI may conduct investigations to follow up personal data matters. Regarding telecommunications, the IFT is in charge of this sector.

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?

The Applicable Laws are silent in this regard.

Begoña Cancino
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Tamarindos 60
Bosques de las Lomas
Mexico

Tel: +52 55 4748 0679
Email: begona.cancino@creel.mx
URL: www.creel.mx

Begoña Cancino is a partner in the Mexico City office. Her practice focuses on Intellectual Property, Data Privacy, Regulatory and Administrative Litigation. From the standard IP front, Ms. Cancino counsels clients from all kinds of industries with the protection and enforcement of their IP rights in Mexico, assisting also with the transfer of IP portfolios within the context of complex corporate transactions involving all sort of IP rights (such as trademarks, copyrights and appellations of origin). Ms. Cancino also provides assistance with her legal advice on regulatory and advertising, assessing our clients to comply with all applicable provisions with COFEPRIS and PROFECO. She has represented clients in all sort of administrative litigation proceedings, in general, concerning advertising, health, environmental and, of course, IP matters, before administrative authorities and federal judicial courts. Pursuant to the data privacy aspects, Ms. Cancino has counselled clients from multiple industries in the drafting and implementation of internal policies, privacy notices and specific legal concerns, not only regarding client daily operations, but also within the context of cross-border transactions and internal investigations for compliance.

Oscar Arias
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Tamarindos 60
Bosques de las Lomas
Mexico

Tel: +52 55 8525 1953
Email: oscar.arias@creel.mx
URL: www.creel.mx

Oscar Arias is an associate at Creel, García-Cuéllar, Aiza y Enríquez S.C., where he specialises in Intellectual Property and Data Privacy. Mr. Arias' experience includes obtaining registrations and protection of all sorts of Intellectual Property rights, as well as the negotiation of technology transfer, technical assistance, licence, and franchise and settlement agreements. He has also worked on Intellectual Property litigious matters – infringement, nullity and cancellation actions – with regard to trademarks, slogans, trade names, industrial designs, copyrights and patents, particularly in the pharmaceutical field. Additionally, he has participated in the litigation and consultancy of health regulations and public acquisitions.

CREEL GARCÍA-CUÉLLAR AIZA Y ENRÍQUEZ

Creel, García-Cuéllar, Aiza y Enríquez is an award-winning, full-service corporate law firm. It has over 80 years of experience in providing international and domestic clients with technical excellence, knowledge of the market and unparalleled client service. The firm is a strategic service provider to clients with the most complex and demanding transactions and projects, affording them certainty and peace of mind. The firm provides innovative solutions to many of the largest, most intricate, first-ever market-leading deals in Mexico. We are a full-service corporate law firm, specialising in the following practice areas and industries: antitrust and competition; arbitration and dispute resolution; banking and finance; bankruptcy and restructuring; capital markets; corporate and commercial; employment and labour; energy and natural resources; environmental; infrastructure; insurance and reinsurance; intellectual property; mergers and acquisitions; private equity; *pro bono*; project development and finance; real estate; social security; tax; telecommunications; and transportation.

Current 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
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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