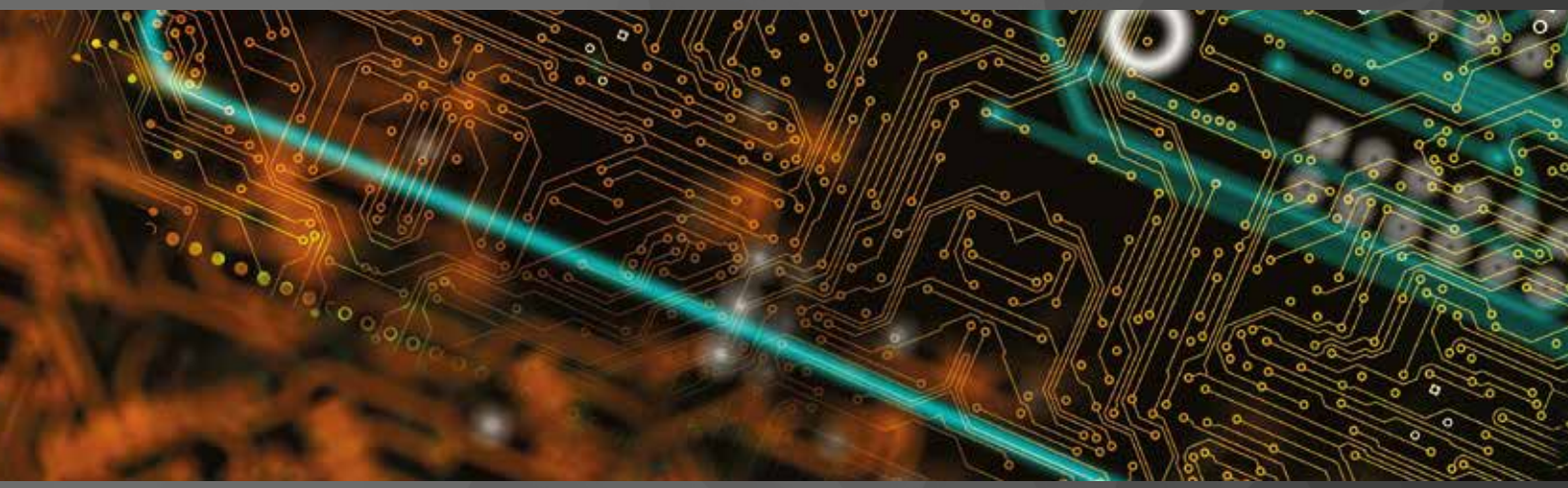
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

United Arab Emirates


Hamdan Al Shamsi


Helen Tung

Hamdan AlShamsi Lawyers & Legal Consultants

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative 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)
The law incriminates hacking and provides various penalties depending on: the way in which electronic information was hacked; the content of what was hacked and what result the hack brought about; and whether information was destroyed or stolen. The basic sentence for accessing an electronic database or software or programme without rights and privileges to do so is imprisonment and a fine of AED 100,000 to AED 300,000. The sentence would be higher if the act affected a government entity or otherwise a company. If the hacking results in any damage, or destroys, amends or deletes any data, the penalty increases to imprisonment for at least six months and a fine of up to AED 750,000.

It should be noted, with the introduction of the DIFC Data Protection Law, No. 5 of 2020 (DIFC DPL), that whilst there are no criminal offences in place, there could well be administrative fines applicable as per Art. 62 as a consequence of a breach. The laws and regulations are administered by the Commissioner and personal data are either kept and/or processed by the Controller or Processor. The onus lies within the remit of the Controller or Processor within an organisation. Such administrative fines are listed in Schedule 2 of the Data Protection Laws, ranging from US$25,000 to US$100,000. It is foreseeable that each breach is likely to be assessed on the facts.

Denial-of-service attacks
Denial of service attacks are punishable under UAE law. They are punishable by a fine of AED 100,000 to AED 300,000 and/or imprisonment.

It should be noted, with the introduction of the DIFC DPL, No. 5 of 2020, that whilst there are no criminal offences in place, there could well be administrative fines applicable as per Art. 62 as a consequence of a breach. See "Hacking (i.e. unauthorised access)" above.

Phishing
If the phishing was directed at obtaining passwords or security information to log in or gain access to systems, then the perpetrator can be subject to jail and/or a fine of between AED 100,000 and AED 500,000. If the perpetrator was able to obtain banking information or credit card information, they would be subject to jail and fines depending on whether they committed the crime to misappropriate money or not. In the case where they had the intention but did not necessarily appropriate the money, they would be subject to a minimum sentence of six months and a fine of between AED 100,000 and AED 300,000. If the perpetrator was able to actually misappropriate money, they would be subject to a minimum sentence of one year's imprisonment and a fine of between AED 100,000 and AED 1,000,000.

It should be noted with the introduction of the DIFC DPL, No. 5 of 2020 that whilst there are no criminal offences in place, there could well be administrative fines that come in place, that come under Art. 62 as a consequence of a breach. See "Hacking (i.e. unauthorised access)" above.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Infecting a server, electronic system or data with any type of malware, virus or program is punishable with a minimum of five years' imprisonment and a fine of between AED 500,000 and AED 3,000,000. The penalty is reduced if the act did not cause any harm or change, or take information.

If such infection results in a breach of the data protection rules in the form of disclosed personal emails and details, then it is likely it would trigger further fines and liabilities as per Schedule 2 of the DIFC DPL.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The distribution, sale or offering for sale of hardware, software and tools could be legal in principle. However, allowing such tools to "commit" cybercrimes suggests that it may well be illegal. Notwithstanding, clearly any breach of the DIFC DPL would result in fines and/or liabilities.

Possession or use of hardware, software or other tools used to commit cybercrime
Any person who creates, sells, markets or otherwise makes available for sale any tools to commit cybercrimes shall be subject to imprisonment and/or a fine of AED 100,000 to AED 500,000. The law also punishes any person who may have a website or database that carries and possesses something illegal with knowledge of its illegality or who has not removed it after being directed to do so by the authorities.

Identity theft or identity fraud (e.g. in connection with access devices)
Any person found guilty of fraud, using someone's identity for his own benefit, will be subject to a minimum of one year's imprisonment and a fine of between AED 150,000 and AED 1,000,000.

Moreover, the DIFC DPL raises the importance of personal data, thereby giving rise to greater responsibility for companies, especially those designated as Controllers/Processors, to ensure there is consent. Hence in scenarios where such consent is not present, and the data is breached, one can envisage fines/liabilities flowing from that.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Any person who obtains and uses confidential information illegally, through his employment, can be subject to imprisonment for a minimum of six months and a fine of between AED 500,000 and AED 1,000,000.

Moreover, the DIFC DPL raises the importance of personal data, thereby giving rise to greater responsibility for companies, especially those designated as Controllers/Processors to ensure there is consent, and hence in scenarios where such consent is not and moreover, their data is breached, one can envisage fines/liabilities flowing from that.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
This is a difficult question, because the ultimate question in the context of the DIFC DPL is whether there is consent at the time the information is supplied. If such unsolicited penetration testing would preclude divulgence of such personal data, whether or not it is part of a simulation exercise, then arguably one could say no harm was done.

If, however, such unsolicited penetrating testing results in data being released to the public, with or without the person's consent, then there may be a broader issue as to breach of the DIFC DPL rules, which may result in fines/liabilities the extent of which would most likely require assessment on a case-by-case basis.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
There are many additional crimes listed that are punishable under UAE law, including intercepting any correspondence or calls and recording them. Other crimes punishable include blackmailing using the internet or through other electronic means, insulting or verbally assaulting anyone using electronic means, money laundering, using any electronic means for terrorism and collecting any charity without a licence to do so. It is punishable by law if electronic means are used to threaten the security of the country.

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

The law does have extra-territorial application for any breaches of the law by any offenders, except in connection with a database or electronic property related to the government or its departments.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Currently, there appears to be none. In fact, if we were to look at the DIFC DPL, there appears to be greater opportunities for development and scope especially when we look at the Codes of Conduct (Art. 48) and potential Certification Schemes. It would be fair to say that there is no current accepted standard under which such "ethical hacking" can be accepted; however, that is not to say that may not change in the near future.

2 Cybersecurity Laws

2.1 *Applicable Law*: 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, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

The laws that relate to cybercrime are Cybercrime Law no. 5 of 2012, replacing Cybercrime Law no. 2 of 2006, and the DIFC DPL 2020.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

It would be useful to see where the DIFC DPL does not apply, including in personal or household activity that has no connection to a commercial purpose. If that were the case, and assuming critical infrastructure and operators of essential services have a commercial purpose, then on the face of it the DIFC DPL would apply. To what extent, and what legal ramifications apply, would most likely need to be assessed on a case-by-case basis.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

There are no laws that require organisations to take measures to monitor, detect, prevent or mitigate cybercrimes; however, regulators in certain industries will set out regulations to require organisations to deal with cybercrimes and prevent them. One example of such is the central bank, which issues circulars and instructions to banks for dealing with cybercrimes.

To the extent that any incidents give rise to breach of the DIFC DPL, then it may well be recommended that organisations have a plan to address such issues. For example, under Part 7 of the DIFC DPL, there is a requirement for any personal data breaches to be notified to the Commissioner and Data Subject, so it would be advisable for organisations to have a plan of action ready in case such breaches were to occur.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) 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; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

(a) In the context of the DIFC DPL, the circumstances would most likely be a breach of personal data in some shape or form.
(b) The Commissioner would need to be notified as well as the Data Subject.
(c) Presumably, basic information, depending on the circumstances/impacts and consequences.
(d) Under the DIFC DPL, there are certain provisions if the Data Subject had withdrawn their rights, or attempts have been made to contact them that such further information ought to be taken into account.

2.5 *Reporting to affected individuals or third parties*: 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 Art. 42 of the DIFC DPL, there is an obligation to notify the Data Subject if it is likely there is a high risk to the security or rights of the Data Subject. The key phrase is "high risk", which may well mean that there is a chance, yet the event has yet to occur, which means that the burden is placed on the company with such information.

The nature and scope of scope of such information would need to be provided in clear and plain language and, where possible, recommendations ought to be made to mitigate any potential adverse effects.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The Commission is in charge, who is appointed by the President. The President shall consult the DIFCA Board of Directors in that regard (Art. 43 of the DIFC DPL).

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Fines/liabilities can be imposed. Please see Schedule 2 of the DIFC DPL.

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

The question of enforcement is not stated explicitly; however, there is reference under Art. 59, which refers to "seek[ing] Judicial Review by the Court", which presumably allows for appeal or assessment of how the law is applied. It is yet to be seen whether such decisions are enforceable.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Beacons may be used; however, if by using the beacon information an IP address is obtained and such was used for committing a crime, then it would not be allowed, and it would be considered illegal.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Honeypots are permitted.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
If it is used only for the organisation's own IP addresses, then sinkholes are permitted, but if it happens to result in diverting traffic away from other organisations then it may breach cybercrime law.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

To the extent that there may be a breach and mitigation is required, one can safely presume the answer is yes; however, the circumstances would be very limited.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Such import/export is likely to be assessed on a case-by-case basis.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice differs from one industry to another. As explained, different industries have different regulators, who may have requirements and instructions to companies in that specific industry.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The financial sector is regulated by the central bank of the UAE. The central bank issues circulars that may include instructions for banks to deal with cybersecurity. The telecommunications sector is regulated by the Telecommunications Regulatory Authority (TRA), which may communicate certain instructions to them too. Whilst there may not be any laws specific to these sectors, the regulators and authorities may communicate instructions to the companies in such industries.

5 Corporate Governance

5.1 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' or officers' duties in your jurisdiction?

Managers and directors can be found liable under the laws of the UAE. This is dealt with in the general rules of responsibility for damage caused (tort) and other articles that deal with the responsibilities of managers and board of directors towards their companies. Managers and directors who may be seen to have omitted or acted in a wrongful way, which caused harm to a company, may find themselves liable for losses and damages.

With the DIFC DPL, the role of a Controller/Processor is important to the extent that a fine may be imposed. It is anticipated that, as the law is still in a nascent stage, through case law and evolution of practice, we are yet to see what the best practices are. Currently, the DIFC DPL makes clear what potential fines and liabilities companies may be subject to and so it gives a sense of what and the seriousness of any breach could result in significant financial penalties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (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?

Companies generally are not required to appoint a CISO and neither do they have to by law establish an incident response plan or policy, conduct periodic cyber risk assessments or perform tests unless required and instructed by a regulator for a specific industry; for example, the central bank or the TRA.

However, in the context of the DIFC DPL, the approach very much relies on the Controller/Processor in ensuring details are captured, processes are in place and therefore quite naturally one can see assessments and performance penetration tests or the like being performed. The new law gives impetus to organisations to think proactively rather than reactively in how to tackle and prevent data protection breaches.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There is no law requiring such disclosures; however, certain regulators may have instructed companies in certain industries to do so, save for in relation to the DIFC DPL.

6 Litigation

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

Any civil action may be brought if a claimant can prove that an act through the internet or electronic means caused harm to the claimant. The claimant would need to prove causation and damages.

In relation to the DIFC DPL, there are directions under Art. 59 which allow for complaints to be addressed to Commissioners. It is still too early to understand how this would work on a practical level, though it is safe to say that should reasonable measures be taken, then matters could potentially be resolved. If not, we may see new developments via case law.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

There are no incidents that can be disclosed.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

The UAE has a concept similar to tort in which a claimant may claim against any person who, through such act, caused harm to a claimant. Such a concept would apply to incidents in cyberspace.

Under the DIFC DPL, there are fines/liabilities as per Schedule 2.

7 Insurance

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

Yes, they are permitted.

7.2 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?

There are no limitations. Insurance companies may exclude or

include clauses in their policies with insured persons. There are no legal limits for these types of insurance cover.

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.

By law, the authorities have certain powers in relation to cybercrimes, including contacting service providers for information, requesting access to information, reviewing information and other general powers of investigative bodies. Likewise, in relation to the DIFC DPL, the Commissioner has a right to conduct such investigations.

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 requirements for such; however, the authorities may, by law and as part of their mandate, instruct and require cooperation from persons in the country. However, it may well be in the interests of companies to consider implementing backdoors, as the fines/liabilities for any breach of the DIFC DPL are not insignificant.

Hamdan Al Shamsi has built one of Dubai's most reputable and respected law practices, and is widely regarded as a top litigator in the Dubai Courts with immeasurable experience in corporate, banking & finance, and insurance law. Hamdan advises both local and international companies as well as governmental entities in cases involving complex litigation. He appears regularly before both the Appeals Court and the Court of Cassation, as well as the UAE's Federal Supreme Court.

Hamdan AlShamsi Lawyers & Legal Consultants
Office 107
Bay Square, BLD- 07
Marasi Drive, Business Bay, Dubai
United Arab Emirates

Tel: +971 4 346 9262
Email: hamdan@alshamsilegal.com
URL: www.alshamsilegal.com

Helen Tung, LL.B. (Hons) is a UK-trained Barrister with 11 years of post-qualification experience. Helen attended the University of Sheffield, Tilburg University and the University of Law, where she obtained her law degrees. Helen furthered her studies at the University of Greenwich for Ph.D. studies (completed coursework only) in maritime security and international law and undertook Directed Studies on International Private Law at The Hague Academy.
Helen works in the DIFC department, specialising in commercial disputes including banking, bankruptcy, construction, and shipping.
Prior to joining HAS, Helen worked in reinsurance, maritime law and commercial disputes in London and advised clients globally. Helen also had experience working as a policy legal advisor for the UK Maritime Coastguard, was an advocate for the Home Office with experience in the Court of Appeals and had secondments with leading shipping law firms in Seoul and Shanghai. Helen has also advised the European Commission, METI and UAE Space Agency in relation to space law and policy.
Helen is a member of the Dubai Courts of the Future Working Group, a founding member of the Maritime Autonomous Regulatory Systems Working Group (MARSWG) and a member of the SmartShip ISO standards committee. Helen is also a committee member of the Knowledge Management group of the International Bar Association addressing the role of AI and emergent technologies in law.
Helen is also part of 7 Pillars law working in space law, and the Founder of NewSpace2060.

Hamdan AlShamsi Lawyers & Legal Consultants
Office 107
Bay Square, BLD- 07
Marasi Drive, Business Bay, Dubai
United Arab Emirates

Tel: +971 4 346 9262
Email: htung@alshamsilegal.com
URL: www.alshamsilegal.com

Established in 2011, Hamdan AlShamsi Lawyers & Legal Consultants has adapted and expanded, paving the path for our diverse range of legal experience and clientele. Based in the UAE, our legal practice provides sector expertise at both the local and international levels. Hamdan Al Shamsi is not only known for his successful cases that have been internationally recognised, such as the Al Khorafi Swiss Banking accomplishment, but also his litigation expertise and especially copyright experience. Hamdan is known by reputation throughout the UAE for not only his position as Senior Partner of leading firm Hamdan AlShamsi Lawyers, but also as the CEO, heading a team of international lawyers. The firm's areas of legal litigation and consultancy expertise include, but are not limited to: Banking & Finance; Construction; Corporate, Criminal; Family; Maritime; Employment (Labour); Real Estate; and Intellectual Property Law.

www.alshamsilegal.com

HAMDAN ALSHAMSI
LAWYERS & LEGAL CONSULTANTS

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
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
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group