ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

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.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

New Zealand

Wigley & Company

Michael Wigley

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Privacy Act 1993 is the principal data protection legislation.

1.2 Is there any other general legislation that impacts data protection?

No, save for the public sector (see question 1.3). However, the common law (the Judge-made law) is important. For example, the Privacy Act has limited application to parties other than natural persons such as companies.

There are common law remedies available from the courts relating to duties of confidentiality, tort claims such as in privacy and negligence, and contract claims where contracts are breached as to data.

There is some related new legislation. The Harmful Digital Communications Act 2015, which deals with cyberbullying and other forms of online harassment and intimidation, brings in a range of measures to address damaging electronic communications spread through methods such as emails, texts and social media posts.

1.3 Is there any sector specific legislation that impacts data protection?

The public sector has legislation applicable to the information it holds, including the Official Information Act and the Public Records Act. The Privacy Act contains provisions specific to the public sector such as in relation to information sharing between public sector agencies. This chapter focuses on the private sector.

There is legislation that touches on privacy issues. In addition, the Privacy Commissioner has issued specific binding codes for industries and sectors such as health, credit reporting, and telecommunications. These codes principally amend the IPPs described in section 3 below to apply to those sectors.

1.4 What is the relevant data protection regulatory authority(ies)?

The Privacy Commissioner, whose office is called the Office of the Privacy Commissioner (OPC), is the relevant data protection regulatory authority.

The Ombudsman has a role also in regard to the public sector.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Although the Privacy Act implements the OECD Guidelines, the definitions differ from, say, the EU provisions. Therefore, there are no definitions similar to, for example, 'data processor'. The reason for this is that the Privacy Act revolves around broadly stated principles called Information Privacy Principles (IPP).

  The key definitions are in s 2, Privacy Act:

  - **"Personal Information"**

    This means information about an identifiable individual, that is, a natural person other than someone who has died. The Privacy Act therefore does not deal with information about companies and other entities, although such information can sometimes also be about individuals.

  - **"Agency"**

    An agency is the party responsible for appropriately dealing with personal information. The agency is any party (including individuals, companies, public and private sector, etc.), with some exceptions (for example, news media are excluded in relation to news activities).

- **"Sensitive Personal Data"**

  This is not applicable.

- **"Processing"**

  This is not applicable.

- **"Data Controller"**

  This is not applicable.

- **"Data Processor"**

  This is not applicable.

- **"Data Subject"**

  This is not applicable.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  There are no other key definitions in particular.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The Privacy Act revolves around a series of 12 Information Privacy Principles or IPPs. They are, at present, outlined at a high level, although the nature of the IPPs is that they are broadly based principles rather than being detailed and prescriptive. Decisions and guidance in relation to the IPPs, particularly from OPC and the Human Rights Review Tribunal, are helping clarify over time how the IPPs apply in particular contexts. For example, the manner and extent of permitted video camera surveillance is clarified by decisions made over time.

  There are some carve-outs in the IPPs. For example, many IPP requirements will not apply when the affected individual consents to different treatment. In keeping with its broadly principled approach, rather than prescriptive detail, the Act is not specific about how that consent is provided such as opt-in or opt-out. Therefore, this is to be decided on the circumstances of the matter.

  Another example is that a number of the IPPs permit disclosure of personal information so long as the individual cannot be identified (e.g., in statistics).

  Also, on particular issues, other legislation may trump the Privacy Act.

  Pivotal to the IPPs are the definitions, outlined above, of "personal information" (broadly, any information about an identifiable individual) and "agency" (broadly, any person, company, public sector agency, etc., that holds personal information).

  The IPPs at a high level are:

  - **IPP1**: Purpose of collection of personal information: Personal information is not to be collected by an agency unless for a lawful purpose connected with the agency and collection is necessary for that purpose.
  - **IPP2**: Source of personal information: The agency must collect personal information from the individual concerned, unless exceptions apply (e.g., individual consents, information publicly available, compliance is impractical, information will not be used in a form whereby the individual can be identified, etc.).
  - **IPP3**: Collection of information from subject: Where personal information is collected from the individual concerned, the agency must take such steps as are reasonable in the circumstances to ensure that the individual is aware of: the collection; the purpose for collection; intended recipients; contact details for the agency; and the individual's right to access to the information and to have it corrected.
  - **IPP4**: Manner of collection of personal information: Personal information is not to be collected by the agency by unlawful means or by means that in the circumstances are unfair or unreasonably intrude on personal affairs of the individual.
  - **IPP5**: Storage and security of personal information: An agency that holds personal information must ensure:
    - that the information is protected, by such security safeguards as are reasonable in the circumstances, against loss, misuse, access, disclosure, etc.; and
    - that if it is necessary to give the information to a party that is providing a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.
  - **IPP6**: Access to personal information: When an agency holds readily retrievable information, the individual concerned shall:
    - be able to obtain confirmation from the agency as to whether such information is held;
    - have access to that information; and
    - if the individual does get access, shall be informed of his or her rights under IPP7.
  - **IPP7**: Correction of personal information: Where an agency holds personal information, the person concerned can request:
    - correction of the information; and
    - that a statement is attached to the information stating that a correction was requested but not made.
  - **IPP8**: Accuracy, etc., of personal information to be checked before use: An agency shall not use personal information without taking such steps as are reasonable in the circumstances to ensure that the information is accurate, up to date, and not misleading.
  - **IPP9**: Agency not to keep information longer than necessary: The agency must not keep the information for longer than required for the purposes for which it can lawfully be used.
  - **IPP10**: Limits on the use of personal information: An agency that has collected personal information for one purpose must not use that information for another purpose (unless an exception applies such as: consent; the second purpose directly relates to the first purpose; and the information is used in a form in which the individual is not identified).
  - **IPP11**: Limits on disclosure of personal information: An agency holding personal information shall not disclose it to another party unless the agency believes on reasonable grounds that, for example, such disclosure is directly related to one of the purposes in connection with which the information was obtained.
  - **IPP12**: Unique identifiers: This IPP provides that no agency shall assign a unique identifier to an individual unless this is necessary for the agency to carry out its functions efficiently. Additionally, a unique identifier is not to be assigned by an agency that is the same as the unique identifier assigned by an unrelated agency. The agency must take reasonable steps to ensure that the identifier is assigned only to individuals whose identity is clearly established.
- **Lawful basis for processing**

  This is not applicable.
- **Purpose limitation**

  This is not applicable.
- **Data minimisation**

  This is not applicable.
- **Proportionality**

  This is not applicable.
- **Retention**

  This is not applicable.
- *Other key principles – please specify*

  There are no other key principles in particular.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Generally, individuals have access: see IPP6 above.
- **Correction and deletion**

  Generally, individuals can seek correction, which include deletion: see IPP7 above.
- **Objection to processing**

  If any of the IPPs are breached, including how information is processed, the individual has remedies including complaint to OPC and, ultimately, by seeking restraining orders and damages from the Human Rights Review Tribunal (HRRT). Those claims can be brought via OPC and a prosecuting agency associated with the HRRT, or brought by the individual concerned.
- **Objection to marketing**

  If any marketing does not comply with the IPPs, the individual has the remedies as in 'Objection to processing'. For example, if an agency has collected information for one business area, but then used that information to send marketing material to the individual on another business area, and consent had not been given, this will often be in breach of IPP10.
- **Complaint to relevant data protection authority(ies)**

  See above. The individual can complain to OPC and can also seek remedies, directly or via OPC from the HRRT.
- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no such circumstances.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

This is not applicable.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

This is not applicable.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

This is not applicable.

5.5 What are the sanctions for failure to register/notify where required?

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

This is mandatory for each agency. This person is called a Privacy Officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not clear. If an agency fails or refuses to comply with the lawful requirement of the Privacy Commissioner, this is an offence. There is a question as to whether this applies to failure or refusal to appoint a Privacy Officer. A party such as the Privacy Commissioner might be able to get a court order requiring the agency to comply.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

There are none.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

By law, the Privacy Officer encourages and ensures compliance with the Privacy Act by the agency, deals with requests made to the agency under the Act, and works with OPC in relation to investigations.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No, this is not the case.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

The Unsolicited Electronic Messages Act 2007 restricts unsolicited electronic commercial messages such as emails and SMS messages. The restrictions do not include post or phone calls.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes, they are.

7.3 Are companies required to screen against any "do not contact" list or registry?

No, companies are not required to screen against any "do not contact" list or registry.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

A pecuniary penalty up to NZ $200,000 for individuals and NZ $500,000 for organisations, in addition to damages and compensation, are the maximum penalties.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

New Zealand does not have cookie-specific legislation such as is required by the EU Directive. However, the Privacy Act and its IPPs are applicable, and may mean that use of a cookie is not permitted, or only permitted if, for example, there is an opt-in or opt-out notice on the website, depending on the circumstances. IPPs 3, 4 and 10, as described at section 3, are particularly relevant.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

There is no statutory clear delineation, and this falls to be assessed in each case under the IPPs.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

We are not aware of any action.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

The Privacy Act liabilities apply (that is, the Human Rights Review Tribunal can order damages).

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

The general IPPs may, in effect, restrict transfer of some data offshore.

As to specific trans-border data, in 2010, the Privacy Act was amended to add the ability for the Privacy Commissioner to prohibit a transfer of personal information from New Zealand to another State, where he or she reasonably believes that:

- the information has been or will be received from another State, and is likely to be transferred to a third State without comparable privacy/data protection legislation to the New Zealand Privacy Act; and
- the transfer is likely to contravene the basic principles of national application in Part 2 of the OECD Guidelines on privacy and trans-border flows of data. In deciding what to do, the Commissioner has regard to a number of factors, including the OECD Guidelines and the EU Directive 95/46/EC.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

In practice, the main consideration will be whether the transfer will comply with the IPPs, and this is fact-specific. For example, under IPP5, will transfer of data to an offshore cloud service provider meet the obligation on the New Zealand agency to ensure that everything reasonable is done to prevent unauthorised use or disclosure of the information? This will depend on various facts such as the sensitivity of the information, the contract with the cloud service provider, what security steps it has taken, etc.

The issue under the OECD Guidelines will arise, but generally not for companies.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

No, this is not the case.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There are no specific requirements for hotlines.

However, to get the protection of the whistle-blower legislation (the Protected Disclosures Act), the whistle-blower needs to have a reasonable belief that there is 'serious wrongdoing' which includes:

- unlawful, corrupt or irregular use of public money or resources;
- conduct that poses a serious risk to public health, safety, the environment or the maintenance of the law;
- any criminal offence; or
- gross negligence or mismanagement by public officials.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

No, this is not the case.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

No, this is not the case.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

This is not applicable, as there is no hotline legislation.

9.5 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

This is not applicable.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies)?

No, this is not the case.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Like many issues under the Privacy Act, this comes back primarily to application of the IPPs, and this is dependent on the facts in each case. If notice is given, or consent obtained, the ability to monitor is likely to be compliant. Generally, absent special circumstances, surveillance in areas such as lavatories would not be compliant.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

As noted above, where there is consent or notice, the monitoring will generally be more likely to be compliant. The adequacy of the type of consent (opt-in or opt-out, etc.) or notice (e.g., the prominence of the notice) will depend on the circumstances. Ideally, written opt-in consent is obtained.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

There is no specific requirement, but consulting those representatives may in some circumstances make it more likely that there will be compliance.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No, this is not the case.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes. IPP5, described in section 3 above, is the most relevant provision in the Privacy Act. When an agency gives personal information to a third party provider such as a cloud service provider, it must do everything reasonably within its power to prevent unauthorised disclosure or use of the information. The level of the requirement in this regard will depend on the facts such as the sensitivity of the data, the security and other protection provided by the cloud provider, the contractual terms, the country where the data will go, etc. If the data is particularly sensitive (e.g., health records), the agency will need to be particularly careful and consider doing due diligence, etc. Many multi-national cloud provider contracts currently fall short.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

For the reasons outlined in question 11.1, there are no specific contractual obligations. Rather, as part of the overall circumstances, the contract will need to be sufficiently robust. This is just one of the requirements to be considered.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes. Even if the Big Data is sourced from personal information about an identifiable individual, if the information is anonymised so that the individual can no longer be identified, this is acceptable. However, there is an increasing risk, internationally, that data like this can be matched in such a way that the individual can be identified.

If Big Data analytics are used for purposes that do identify the individual (for example, to market to that person), there must be compliance with the IPPs outlined at section 3 above. For example, it may not be possible to use some information to market to the individual if he or she has not consented. Typically, therefore, companies will get customers to sign up to consent (such as when getting loyalty cards), permitting use of data in this way.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no statutory minimum requirements such as obligations to comply with certain international standards. IPP5, described at section 3 above, is, as is often the case for companies, at the heart of their obligations. Agencies must have security safeguards that are reasonable in the circumstances. Health and banking records require high levels. Pizza orders require lower levels. If an agency follows and applies best industry practice in terms of security, such as compliance with international standards, modern security practices, etc., the risk of non-compliance is more likely to be low.

As noted at the outset, there can be other sources of liability such as negligence, breach of confidence and contract, etc. They are important considerations, especially for companies and also for B2B dealings.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

No. The Privacy Commissioner might prefer to have voluntary disclosure, but this is not currently enforceable.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

No, and the position is the same as in question 13.2.

13.4 What are the maximum penalties for security breaches?

Beyond compensation under the general common law or the Privacy Act, there are no penalties.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Privacy Commissioner	Power to request prosecution official associated with Human Rights Review Tribunal to bring proceedings in that Tribunal.	There are none.
Human Rights Review Tribunal	Orders such as declarations and damages for breach of the Privacy Act, at the instigation of the affected individual or the Privacy Commissioner via the path noted above.	There are none.
Courts	Privacy Act issues do arise in civil court matters, in addition to remedies under the general law such as the tort of negligence and of privacy, the duty of confidentiality, and for breach of contract.	Offences under the Privacy Act.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Privacy Commissioner will generally endeavour to resolve complaints short of taking enforcement action involving proceedings in the Human Rights Review Tribunal. It may, for example, seek voluntary compliance, a mediated settlement between parties, etc. Human Rights Review Tribunal actions in this area are relatively infrequent, and the courts have also dealt with Privacy Act issues on a relatively infrequent basis.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

How to handle such requests will depend on the country where the requests come from and the nature of the requests, plus other factors

such as whether the company or the holding company of the New Zealand entity has an office in the requesting country. If it does, this may raise compliance issues in the requesting country's courts. There are particular rules between Australia and New Zealand. Therefore, for foreign civil discovery, each case should be checked legally.

As to requests for disclosure from foreign law enforcement agencies, again this should be checked carefully. New Zealand is currently receiving international attention in this area, due to the FBI requests to obtain information held in relation to internet entrepreneur Kim Dotcom.

15.2 What guidance has the data protection authority(ies) issued?

There is none.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There are no particular enforcement trends emerging, other than a decision by the Privacy Commissioner to start a "name and shame" regime, by which agencies that appear to be in breach of the data protection legislation may be named publicly. Given the reputational implications for agencies holding data, this is a powerful weapon in the regulator's arsenal. So far, it has not been frequently used but increased activity is more likely going forward.

16.2 What "hot topics" are currently a focus for the data protection regulator?

As in many other countries, whether or not to introduce mandatory breach reporting is under review by Government (this would require amending legislation), although there are indications that this may not happen in New Zealand in view of lack of Government appetite to go down this path.

At present, internationally "hot topics" are getting focus by the regulator in New Zealand too, such as cyber breach, big data, drones, etc.

Michael Wigley
Wigley & Company
Level 6, 23 Waring Taylor Street
Wellington 6011
New Zealand

Tel: *+64 27 44 53 452*
Email: *michael.wigley@wigleylaw.com*
URL: *www.wigleylaw.com*

Michael has been involved in many high-profile projects in New Zealand from large IT projects to most regulatory disputes in telecommunications. Michael has been offering advice on online and internet matters since the early days of the internet, along with IT and telecommunications expertise, and also does dispute and court work. Michael has advised numerous Government departments and companies on data protection issues.

Wigley & Company is a law firm based in Wellington and Auckland, specialising in competition and regulatory law, IT, internet, telecommunications, media, public law, and data protection issues. The firm acts for a wide range of corporates from SME to listed, and for NGOs. It has considerable experience in complex issues requiring lateral and strategic solutions across a range of issues from contract to litigation, from economics to seeking legislative and regulatory change.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- 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 Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

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

www.iclg.co.uk