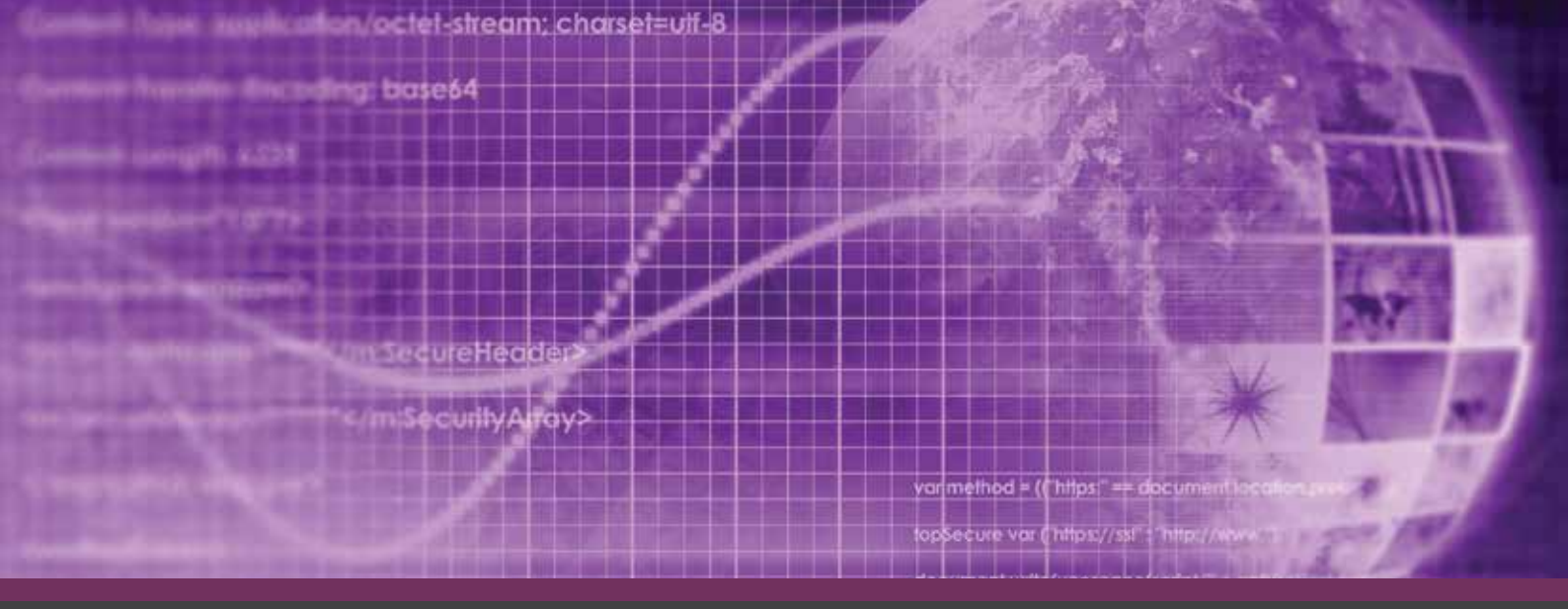

ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Head of Business Development
Dror Levy

Sales Director
Florjan Osmani

Commercial Director
Antony Dine

Account Directors
Oliver Smith, Rory Smith

Senior Account Manager
Maria Lopez

Sales Support Manager
Toni Hayward

Sub Editor
Amy Hirst

Senior Editor
Suzie 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.
May 2015

ISBN
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

China

Manuel E. Maisog

Hunton & Williams LLP Beijing Representative Office

Wei Zhang

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There is no comprehensive, consolidated data protection law in China.

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

The *P.R.C. Constitution* establishes an individual's right to dignity, which under relevant rules is further interpreted to include a right of privacy. The *P.R.C. Constitution* also establishes an individual's right of freedom and secrecy of correspondence. The Tort Liability Law explicitly protects the right of privacy, and allows private rights of action for invasions of privacy. The *Decision on Enhancing Internet Information Protection* protects personal electronic data which is collected and transferred through the Internet. In addition, a consumer's personal information is protected under the *Consumer Rights Protection Law*. Finally, a draft *Counter-Terrorism Law* may have impact on the personal data of domestic telecommunications and Internet users.

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

In China, personal data protection rules are scattered among various sector-specific Chinese laws and regulations. For example, personal financial information has extensive protection under banking sector regulations, and the telecommunications sector has its own rules protecting the personal information of telecommunications service users.

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

There is no particular data protection regulatory authority. Government agencies may act as regulatory authorities in the particular industry sectors under their respective oversight.

2 Definitions

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

- **"Personal Data"**

  There is no clear, single and fundamental definition of "personal data". However, generally speaking "personal data" refers to information which relates to an individual and which either (1) can independently identify the individual, or (2) may be used to identify the individual when combined with other information.

  As one example, a regulation of the State Administration for Industry and Commerce defines "consumer personal information" as "information collected by an enterprise operator during the sale of products or provision of services, that can, singly or in combination with other information, identify a consumer". The regulation then provides a list of specific examples: a consumer's "name, gender, occupation, birth date, identification card number, residential address, contact information, income and financial status, health status, and consumer status". While this is only one regulatory definition among several, given the everyday ubiquity of consumer personal data, this particular definition could prove useful as a rule of thumb for developing a practical understanding of what constitutes "personal data" in China. Definitions provided for other industry-specific regulations can, however, be even more broadly stated than this one.

- **"Sensitive Personal Data"**

  There is no definition of "sensitive personal data". However, some sector-specific regulations provide special protections of certain personal data, effectively treating them much like "sensitive personal data". These include personal financial information, disease and medical history, status as a hepatitis B carrier, and others.

- **"Processing"**

  There is no definition of "processing", but in practice it usually may include collection, transmission, use, disclosure, storage, disposal, etc.

- **"Data Controller"**

  There is no definition of "data controller", but the existing data protection rules mainly regulate entities which collect and use personal information.

- **"Data Processor"**

  There is no definition of "data processor".

- **"Data Owner"**

  There is no definition of "data owner".

- **"Data Subject"**

  There is no definition of "data subject", but in practice it usually refers to an individual whose personal data is collected, used or processed.
- **"Pseudonymous Data"**

  There is no definition of "pseudonymous data".
- **"Direct Personal Data"**

  There is no definition of "direct personal data".
- **"Indirect Personal Data"**

  There is no definition of "indirect personal data".

3 Key Principles

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

- **Transparency**

  Although no precise principle is established for the processing of personal data, existing sector-specific data protection rules often require that the data subject be expressly informed of the purpose, method and scope for collecting and using the personal data.
- **Lawful basis for processing**

  There is no requirement of a lawful basis for processing of personal data. Some existing sector-specific data protection rules, however, require that personal information not be illegally or improperly collected, used or transferred.
- **Purpose limitation**

  Existing sector-specific data protection rules, when requiring that the data subject must be expressly informed of the purpose, method and scope for collecting and using the personal data, also imply that the collection and use must not exceed the prescribed purpose and scope.
- **Data minimisation**

  Some existing sector-specific data protection rules require that unnecessary personal data must not be collected.
- **Proportionality**

  There is no data protection rule concerning this principle.
- **Retention**

  Some existing sector-specific data protection rules require that personal data be kept strictly confidential, and not be disclosed, sold or illegally provided to others; that technical measures be taken to ensure data security and to prevent any data leakage or loss; and that in the event of any occurrence or risk of data leakage or loss, immediate remedial measures be taken.

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**

  Some existing sector-specific data protection rules explicitly provide that a data subject may access his/her own personal data.
- **Correction and deletion**

  Some existing sector-specific data protection rules explicitly provide that a data subject may correct mistake(s) concerning his/her personal data. But there is no rule providing a data subject the right of deletion.
- **Objection to processing**

  There is no precise rule providing a data subject the right of objection to processing.
- **Objection to marketing**

  There is no precise rule providing a data subject the right to object to his/her personal data being processed for marketing purposes. But it is clearly provided in the *Consumer Rights Protection Law* that without a consumer's consent or request, or where a consumer explicitly rejects, a company shall not distribute commercial information to the consumer. There is also a regulation imposing rules and restrictions on the use of "spam" emails.
- **Complaint to relevant data protection authority(ies)**

  There are regulatory authorities respectively supervising the enforcement of existing sector-specific data protection rules, but no precise rule providing how a data subject can make a complaint to these authorities.

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?

There is no requirement to appoint a company data protection officer as a general matter. In the banking sector, commercial banks are required to appoint a chief information officer. This position may involve functions that are similar to those of a data protection officer, but it is not mainly responsible for data protection matters. Companies in the postal and courier services sector are required to appoint a "security information officer". Finally, medical institutions are required to establish a separate department and personnel who would normally also have the responsibilities of a data protection officer.

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

This is not applicable.

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.

This is not applicable.

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

The responsibilities of a chief information officer in a bank are to administer the bank's information technology department and to be responsible for information technology, and also to establish a department to be responsible for IT risk management. A postal or courier services company's "security information officer" is responsible for collecting, reporting and handling security information. A medical institution's department and personnel acting in the role of a data protection officer would generally have responsibility for the collection, use and processing of personal medical information.

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

This is not applicable.

7 Marketing and Cookies

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

Under the *Consumer Rights Protection Law*, without a consumer's consent or request, or where a consumer explicitly rejects, a company shall not distribute commercial information to the consumer.

In particular, the *Measures for the Administration of Internet Email Services* require that: (1) emails containing commercial advertisement content shall not be sent to recipients without their explicit consent; (2) such commercial advertisement emails shall be identified by the words "advertisement" or "AD" in the email's subject field; (3) the identity or origin of the email sender may not be intentionally concealed or forged; (4) the email shall provide valid contact methods (including the sender's email address) through which recipients may indicate their refusal of further emails and which should be valid for 30 days; and (5) the sender is required to stop sending such emails when the recipient indicates his/her refusal, unless otherwise agreed by the parties involved.

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

Apparently not. Not much news on the enforcement of such breaches is reported.

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

Under the *Measures for the Administration of Internet Email Services*, the maximum penalty for sending emails having commercial advertisement content is RMB 30,000.

According to the *Consumer Rights Protection Law*, if a business operator infringes a consumer's rights in connection with his/her personal information, it may be required to make correction, receive a warning, forfeit related illegal income and be charged a fine of up to 10 times the illegal income (if there is no illegal income, the fine will be up to RMB 500,000).

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

There is no rule particularly addressing cookies.

7.5 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 rule particularly addressing cookies.

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

There is no rule particularly addressing cookies.

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

There is no rule particularly addressing cookies.

8 Restrictions on International Data Transfers

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

There are no requirements applicable to cross-border transfers as a general matter. However, there are cross-border transfer restrictions that particularly apply to transfers of personal financial, credit reference and health information to places outside of China.

Under a draft *Counter-Terrorism Law*, companies providing telecommunications or internet-related services in China must store data of domestic users inside China.

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

No exemptions are provided to the foregoing restrictions.

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 exemptions are provided to the foregoing restrictions. There is no registration/notification requirement applicable to cross-border transfers of personal data.

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 is no rule on the use of whistle-blower hotlines.

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?

There is no rule on this matter.

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.

There is no rule on the use of whistle-blower hotlines.

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)?

There is no registration/notification or prior approval requirement on the use of closed circuit television.

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

In China, there is no specific rule explicitly addressing employee monitoring. However, employee monitoring may be subject to the following restrictions under Chinese law:

(1) In China, an individual is entitled to a constitutional right to dignity, of which a right of privacy is a part.

(2) The *P.R.C. Constitution* also grants an individual the freedom and secrecy of correspondence.

(3) The *Decision on Enhancing Internet Information Protection* provides broad protections for personal electronic data, by way of which employee personal information is protected.

(4) An employer must keep employees' personal data in confidence. The employer must obtain the relevant employee's prior written consent before disclosing the personal data to a third party.

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

Yes, consent is required. In practice, the consent may be obtained by way of an appropriate statement in an employment contract, or a provision in an employee handbook or workplace rules that each employee is required to acknowledge and accept by way of a signature.

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

There is no requirement to notify or consult with a work council or trade union.

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

There is no registration/notification or prior approval requirement.

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)?

There is no data protection rule specifically concerning personal data in the cloud.

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)?

There is no data protection rule specifically concerning data processing by cloud-based services.

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)?

There is no data protection rule specifically concerning big data and analytics.

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)?

Certain sector-specific data protection rules require a company to take technical measures to ensure data security and prevent any data leakage or loss, and in the event of any occurrence or risk of data leakage or loss, to take immediate remedial measures. However, except in particular sectors, usually there is no detailed and specific rule on what technical measures must be implemented.

For example, the State Administration of Taxation requires a local tax bureau which receives the tax filing data from an individual whose annual income exceeds RMB 120,000 to make sure the data is encrypted during data transfer; and the China Securities Regulatory Commission requires encryption of storage and transfer of user names and passwords kept in the application system of a securities and futures institution.

In addition to personal tax information, detailed or extensive data security standards have been established for the medical, financial, telecommunications and internet, and courier services sectors. However, more generally stated security standards have been established for numerous other industry sectors.

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.

There are no requirements applicable to information security breaches of personal data as a general matter. However, there are specific requirements in relation to the financial, credit reference, telecommunications, postal and tax sectors.

Financial institutions are required to establish a system for reporting major safety incidents and risk events arising in the electronic banking business, and to maintain regular communications with supervisory departments. In situations where the electronic banking system is maliciously damaged, or infected by a virus which results in a breach of confidential information, financial institutions must report to the China Banking Regulatory Commission within 48 hours.

If a serious information leakage accident occurs at a credit reference institution which operates a personal credit information business, at the Basic Database of Financial Credit Information, or at the institution which provides credit information or which makes inquiry with the Database, the administrative authority of the credit information collection sector may take necessary measures such as a temporary takeover in order to mitigate the damages.

In case there is any leakage or possible leakage of telecommunications users' personal information, which has caused or may cause serious consequences, then the relevant Internet information service provider should report such event to the competent telecommunications regulatory agency.

Any company providing postal services or courier services must report to the relevant postal administration authority within 3 days, if an employee opens, hides or discards more than 10 pieces of another person's mail without authorisation.

In the event of any incident in which tax-related confidential information is leaked, the relevant tax agency must report such event in a timely manner according to relevant laws and rules.

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.

There is no such requirement.

14 Enforcement and Sanctions

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

China does not have a particular data protection authority with specific investigatory power(s).

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

This is not applicable.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

There is no particular rule on how companies within China may respond to foreign e-discovery requests for disclosure of personal data.

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.

The most important enforcement trend was the conviction of a British national and his U.S. citizen wife in a criminal prosecution in Shanghai in which they stood accused of the improper collection of personal data. The case raises the question of whether enforcement actions will more consistently be brought against foreign citizens and foreign-invested enterprises for alleged infringements of personal information.

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

There are two at this time: (1) whether, in the wake of the criminal conviction in Shanghai (mentioned above), more enforcement actions will be brought against foreign citizens and foreign-invested enterprises for alleged infringements of personal information; and (2) whether a draft Counter-Terrorism Law, which contains certain provisions that would restrict cross-border flows of information, will be enacted.

Manuel E. Maisog
Hunton & Williams LLP
Beijing Representative Office
517-520 South Office Tower
Beijing Kerry Centre
No. 1 Guanghua Road, Chaoyang District
Beijing 100020, P.R.C.
China

Tel: +86 10 5863 7500
Fax: +86 10 5863 7591
Email: bmaisog@hunton.com
URL: www.hunton.com

Bing Maisog is the Chief Representative of the firm's office in Beijing, and is a principal of the Centre for Information Policy Leadership. His practice focuses on data protection and privacy, energy, finance, mergers and acquisitions, and foreign direct investment. Bing frequently advises clients on existing and emerging privacy and data security laws in the Asia-Pacific region, including with respect to the ongoing development of China's developing data protection framework. He graduated with an undergraduate degree in public and international affairs from Princeton University, and studied law at Harvard Law School.

Wei Zhang
Hunton & Williams LLP
Beijing Representative Office
517-520 South Office Tower
Beijing Kerry Centre
No. 1 Guanghua Road, Chaoyang District
Beijing 100020, P.R.C.
China

Tel: +86 10 5863 7500
Fax: +86 10 5863 7591
Email: weizhang@hunton.com
URL: www.hunton.com

Wei Zhang is an associate in the firm's Beijing office. Her experience includes representation of multinational companies, Chinese state-owned companies and investment banks. She advises multinational companies operating in China on all aspects of privacy and data protection compliance governing the collection, use and processing of personal data in China.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by Computerworld magazine for four consecutive years as the top law firm globally for privacy and data security. Chambers and Partners ranks Hunton & Williams the top privacy and data security practice in its Chambers & Partners UK, Chambers Global and Chambers USA guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among The National Law Journal's "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy, Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

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
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- 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