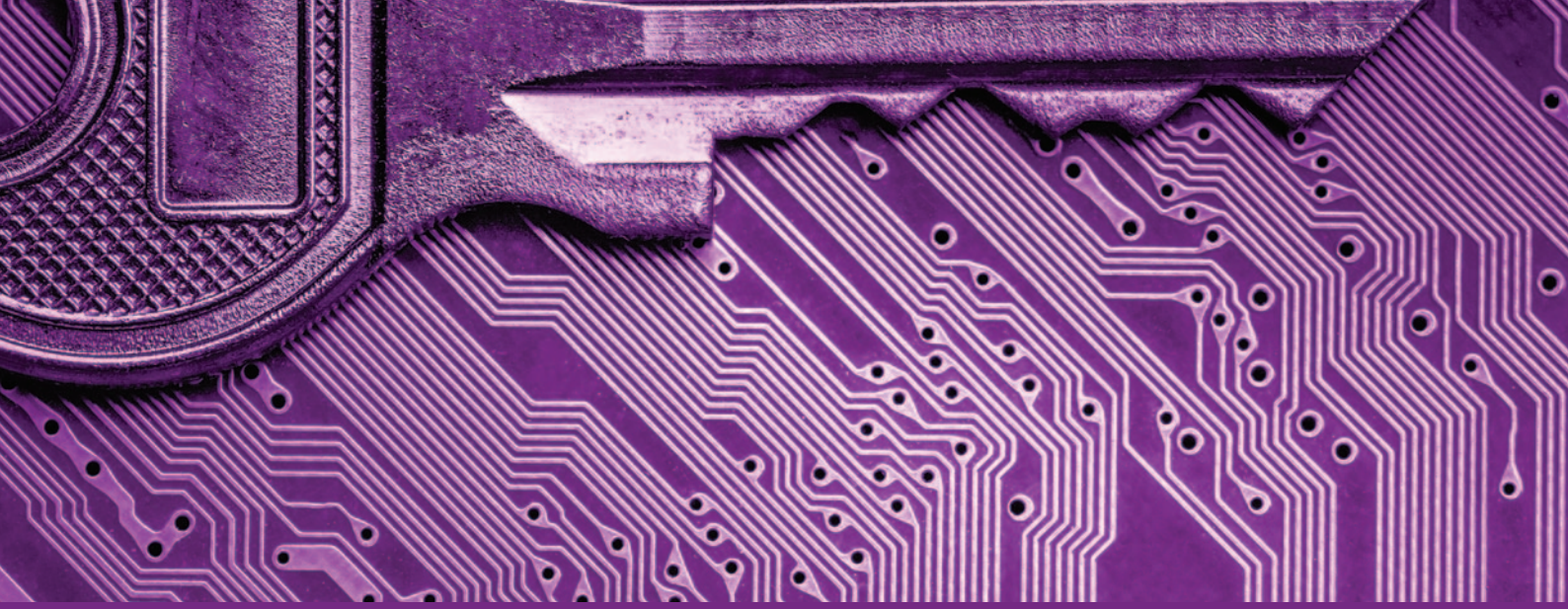

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

Contributing Editor
Tim Hickman &
Dr. Detlev Gabel,
White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
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
June 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Why Should Companies Invest in Binding Corporate Rules?

FABIAN PRIVACY LEGAL GmbH

Daniela Fábián Masoch

1 Introduction

Article 47 of the EU General Data Protection Regulation ("GDPR") expressly recognises Binding Corporate Rules ("BCR") as one of the means for the international transfer of personal data, both for controllers (covering personal data they control) and for processors (covering personal data they process on behalf of others based on a processing agreement). Before the GDPR came into force, BCR were recognised and approved by the current practice of the data protection authorities and the guidelines of the Article 29 Working Party ("Working Party"). Other countries outside of the EU, such as Switzerland, recognise the concept of BCR as well.

What is the practical significance of BCR for companies and why should companies invest in BCR? This article shall explore what BCR under the GDPR are, what needs to be considered when applying and implementing BCR, and their benefits.

2 What are Binding Corporate Rules?

The GDPR defines the term "Binding Corporate Rules" in Art. 4 para. 20 as "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity".

BCR are therefore one of the appropriate safeguards for the transfer of personal data within a group of undertakings, or group of enterprises engaged in a joint economic activity ("Group") from the European Economic Area ("EEA") to countries which do not provide an adequate level of data protection. In practice, BCR are a set of internal rules, standards and processes, such as codes of conduct, that regulate internal data management practices in a binding and consistent manner throughout the Group, with the primary objective to facilitate the free movement of personal data within that Group while ensuring an effective level of data protection. BCR are, however, not intended to be used as a means for allowing cross-border data transfers to companies which are not part of that Group.

The concept and content of the BCR have mainly remained the same under the GDPR, with some minor changes. One significant change is the extension of the group of applicants. While BCR were previously only applicable to groups of undertakings, they are now also open to groups of enterprises engaged in joint economic activities. The term "group of undertakings" is defined in Art. 4 para. 19 GDPR as a "controlling undertaking and its controlled undertakings". However, the term "group of enterprises engaged in a joint economic activity" is not defined in the GDPR. The term is open to interpretation, but may be taken to include a group of independent organisations which have agreed to cooperate, such as joint ventures.

In addition, the list of minimum requirements has been extended to include the contact details of each member of the Group, the description of the principles of privacy by design and privacy by default, the right not to be subject to profiling, the information obligations according to Art. 13 and 14 GDPR, and the details of the persons responsible for training and complaint procedures.

The Working Party provides, in WP 256 (BCR for controllers) and WP 257 (BCR for processors), updated guidelines and very useful tables setting out the elements and principles that controllers and processors should state in their BCR, incorporating the new language in line with the GDPR and the necessary content mandated by Art. 47 GDPR, and making a distinction between what must be included in the BCR and what must be presented to the competent supervisory authority in the BCR application.

BCR must comply with a whole range of requirements, and must contain all elements as set out in Art. 47 para. 2 GDPR, including:

a) the structure and contact details of the group of undertakings or group of enterprises engaged in a joint economic activity, and of each of its members;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

c) their legally binding nature, both internally and externally;

d) the application of the general data protection principles; in particular, purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the BCR;

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decision based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts, and to obtain redress and, where appropriate, compensation for a breach of the BCR;

f) the acceptance by the controller or processor established on the territory of a Member State, of liability for any breaches of the BCR by any member concerned not established in the Union, whereby the controller and the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

g) how the information on the BCR – in particular, on the provisions relating to the general data protection principles, the rights of the data subjects, and the liability for any breaches of the BCR – is provided to the data subjects;

h) the tasks of any data protection officer designated in accordance with Art. 37 GDPR or any other person or entity in charge of monitoring compliance with the BCR, as well as monitoring training and complaint handling;

i) the complaint procedures;

j) the mechanisms for ensuring verification of compliance with the BCR. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such verification should be communicated to the DPO or any other person in charge of monitoring compliance with the BCR, and to the board of the controlling undertaking, and should be available upon request to the competent supervisory authority;

k) the mechanisms for reporting and recording changes to the BCR and reporting those changes to the supervisory authority;

l) the cooperation mechanisms with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications;

m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity, is subject in a third country, which are likely to have substantial adverse effect on the guarantees provided by the BCR; and

n) the appropriate data protection training for personnel having permanent or regular access to personal data.

3 What Should Organisations Consider Before Applying for BCR?

The use of BCR as an appropriate safeguard for international data transfers from the EEA requires the approval of the competent supervisory authority in the relevant jurisdiction following the consistency mechanism set out in Art. 63 and 64 GDPR. The competent supervisory authority will approve the BCR under the condition that:

a) BCR are legally binding and enforceable on the undertakings concerned;

b) BCR expressly confer on the data subjects enforceable rights concerning the processing of their personal data; and

c) BCR comply with the minimum information requirements set out in Art. 47 para. 2 GDPR.

Before applying for BCR approval, an organisation should carefully consider and answer some key questions:

What does the company want to achieve with the approved BCR?

Is the only objective to facilitate the free flow of personal data within the Group? If so, has the organisation considered any alternatives to achieve this objective, such as concluding an intra-group data transfer agreement ("IGDTA")? Alternatively, is the company's goal, besides safeguarding cross-border data transfers, also to achieve and demonstrate accountability and commitment to responsible data use? If so, the organisation should assess whether BCR are the right approach or whether there are other options such as certification or a code of conduct, which might be more suitable for achieving the interests of the organisation.

Which BCR should be implemented?

The organisation must determine if it wants to apply for BCR for controllers or BCR for processors, or both. Depending on that decision, the appropriate requirements must be fulfilled.

What will be the scope of the BCR?

Will the BCR only cover personal data transferred from the EEA within the Group or will they cover all processing of personal data within the Group? This last option would include any data and go far beyond the legal requirements extending the liability and privacy rights. This extension is ultimately a decision that each organisation must take and may be appropriate for organisations that have decided to establish the same set of rules, standards and rights throughout the whole organisation, irrespective of the jurisdiction and legal requirements. The organisation must also determine if it wants to cover all personal data or limit the BCR to only a set of data such as HR or customer data. Finally, the organisation must determine if all members of the Group shall be bound by the BCR or only a selected number of companies.

Which supervisory authority should be the lead authority for the BCR ("BCR Lead")?

The BCR Lead is the authority that acts as the single point of contact with the applicant organisation during the authorisation procedure and the application process in its cooperation phase. The BCR Lead may differ from the "one-stop-shop" lead supervisory authority according to Art. 56 GDPR, which is mainly involved in handling data breaches and investigatory or enforcement activities in cross-border processing operations within the EU. The organisation applying for BCR authorisation must justify the reasons why a particular supervisory authority should be considered as the BCR Lead. The criteria for such justification are set out in WP 263:

a) the location of the Group's European headquarters;

b) the location of the company within the Group with delegated data protection responsibilities;

c) the location of the company which is best placed (in terms of the management function, administrative burden, etc.) to deal with the application and to enforce the BCR in the Group;

d) the place where most decisions in terms of the purposes and the means of the processing (i.e. transfer) take place; and

e) the Member State within the EU from which most or all transfers outside the EEA will take place.

For companies with their head office or principal place of business in the EU, the justification is quite simple. However, how should companies with their registered office outside the EU and without a principal place of business in the EU choose the appropriate supervisory authority and justify their choice? What arguments could be put forward if there is no Member State within the EU from which most or all transfers are made outside the EEA, but such transfers are roughly the same between all entities in the EU? In this case, the organisation may delegate responsibilities to the Group company that is best placed to process the application for BCR on behalf of the Group. This entity should be located in one of the most important countries for the Group with a strong presence and at the same place as the chosen supervisory authority.

Once the organisation has selected the BCR Lead based on the criteria mentioned above, it will submit its application to that supervisory authority. It should be noted, however, that the selected supervisory authority is not obliged to accept the choice if it believes that another

supervisory authority is more suitable to be the BCR Lead; in particular, taking into account the workload and number of pending BCR applications. The requested supervisory authority will share the application with all concerned supervisory authorities to make a final decision on which supervisory authority is appointed as BCR Lead.

It is advisable that the organisation contacts the selected supervisory authority before applying to check whether the supervisory authority is, in principle, willing to act as BCR Lead or whether there may be objections from the supervisory authority; for example, due to lack of resources to deal with the application in a timely manner.

What should the liability system look like?

Art. 47 para. 2f requires the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the BCR by any member concerned not established in the Union. WP 256 and WP 257 provide that, where it is not possible for a Group with particular corporate structures to impose an obligation on a specific entity to take all the responsibility for any breach of the BCR outside of the EU, it may provide that every BCR member exporting data out of the EU on the basis of the BCR will be liable for any breaches of the BCR by the BCR member established outside the EU which received the data from this EU BCR member. Will it be acceptable for the BCR Lead to introduce an alternative liability system in line with the Standard Contractual Clauses? If not, which Group company could take responsibility? What are the options? Clarification on this issue is crucial, especially for companies based outside the EU which do not have their main establishment in the EU. For some organisations, it may not be feasible to allocate responsibility for the payment of damages to a local entity as a result of a breach of the BCR by a Group company outside the EU.

What is the implementation status of the data privacy management programme within the organisation?

Has the organisation already implemented global standards, policies and procedures, and if so, what is the maturity level at the corporate level and throughout the organisation? Where are potential gaps and risks? Depending on the groundwork done and the maturity level of the data protection management programme, the BCR approval process may take a longer or shorter time.

Is the buy-in of key stakeholders secured?

Do key stakeholders, from executive management to key country organisations and functions, offer their buy-in to the process? Stakeholder support requires their awareness and understanding of the need and benefits of implementing BCR, the commitments that each business unit and function must make with BCR approval, and the expectations placed in them. Preliminary discussions and a presentation of the business case to these stakeholders are therefore an essential step before applying for BCR.

Are there sufficient resources and expertise to manage the approval and implementation of BCR?

Is there a team in place to develop the BCR, collect all relevant information, involve the relevant functions, discuss with the BCR Lead and manage the communication and implementation of the BCR across the organisation? This team may consist of a leader and project manager, as well as contributors to critical functions and the most important markets. A properly functioning internal team is crucial to a smooth approval process and implementation throughout the organisation. For smaller companies with fewer resources and expertise in data protection and project management, the involvement of external experts should be considered.

4 What Should Organisations Consider once BCR Approval is Obtained?

The approval of the BCR is an essential step in the whole process. However, the BCR have no practical effect if they are not correctly implemented throughout the Group. Therefore, in parallel to the approval process, it is crucial that the organisation that is responsible for the implementation of the BCR puts in place a concrete and enforceable communication and implementation plan, with responsibilities and reasonable timelines. Here are some suggestions as to what such a plan should contain at the minimum:

A communication plan that sets out who should inform whom, how, when and about what, during the whole process. When applying for BCR approval, all Group companies and functions at the corporate and local level should be informed of the content and impact of the BCR, in particular their obligations, and of the progress of the BCR approval process. They should also be informed of the steps they need to take before approval to best prepare for the implementation of the BCR. Throughout the process, it is also advisable to address possible problems, questions and concerns to ensure the broadest possible support and to prevent serious issues or concerns from arising following the approval of the BCR. In some countries, works councils must also be informed or consulted, and finally, once approved and implemented, all employees who regularly process personal data must be informed and trained. Clear roles and responsibilities must be assigned to ensure appropriate communication at each level of the organisation.

An implementation plan that is addressed to those functions and individuals responsible for implementing the privacy management programme and the BCR – in practice, the data protection officers, managers or champions – and outlines what needs to be done, when and how. The steps may include the preparation by adopting the Group privacy policy framework and implementing the data protection management programme at the local level, signing the BCR and making them binding upon employees, training employees, verifying compliance with the BCR and handling complaints.

Effective BCR require the establishment of an organisation with responsible persons at corporate and local level to implement the BCR and monitor compliance. A person at corporate level should be appointed to maintain an updated list of BCR members, monitor the state of implementation and any changes, and report annually to the supervisory authority.

5 Why Should Organisations Invest in BCR?

In practice, many companies have concluded so-called intra-group data transfer agreements ("IGDTA") covering the cross-border transfer of personal data within their Group. So why should companies go through the effort of implementing BCR when they can achieve the same goal with an IGDTA? Companies with an IGDTA meet the legal requirements for cross-border data transfer. However, they may not benefit from the impact of BCR, which significantly increase awareness and understanding of privacy requirements within the organisation and establish accountability for compliance with data protection requirements in each function and business unit at corporate and local levels throughout the organisation. Also, the

effort required to create an IGDTA that includes the evaluation of all types of data flows, categories of personal data, purposes and safeguards, as well as the recipients of the data, the documentation of this information, the possible translation into the local language and the signing of contracts by all affiliates, should not be underestimated. It requires the involvement of all business units and functions at global and local levels. At the same time, the IGDTA often remains in a drawer after signing and is never considered again. Rarely will companies implement an IGDTA by establishing appropriate policies, procedures, processes and training.

Organisations that develop and implement BCR regularly aim to achieve an appropriate data protection governance structure with uniform standards and processes across the enterprise, and not only to transfer their data legitimately within the Group. With the approval of the BCR by the supervisory authorities, organisations also want to show that they not only take data protection seriously, but also effectively implement the requirements in the company and assume responsibility for compliance with data protection.

BCR are based on a comprehensive and effective data protection management programme with all the elements required to demonstrate accountability. These elements include:

a) a governance structure with leadership and oversight of the data protection programme;

b) a policy framework with policies and procedures to ensure fair and responsible processing of personal data;

c) transparency through appropriate communication to data subjects;

d) risk assessment and management at the programme and data processing level;

e) awareness raising and training of employees and others who process personal data;

f) monitoring compliance with the data protection programme and verification of its effectiveness through regular self-assessments and internal or external audits; and

g) processes to adequately respond to data subjects' rights, complaints and inquiries, as well as privacy incidents, and to enforce compliance with internal rules.

Organisations subject to the GDPR and other stringent data protection acts must establish a comprehensive data protection management programme, including all the elements listed above, to ensure compliance with the applicable requirements and responsible data use. With the implementation of such a privacy management programme, organisations are ready to consider applying for BCR approval in order to benefit from a valid data transfer mechanism, while increasing their commitment to privacy within the company and promoting a culture of responsible data use.

To obtain approval of the BCR and ensure compliance with the commitments that are made with the application, the data privacy management programme must, however, include specific procedures and processes. The organisation must assign responsibilities for the implementation of the BCR to each BCR member; in particular, for binding the company and its employees to the BCR and for publishing notices. It must further establish a complaint handling process, develop awareness-raising and training plans and have a mechanism to implement these plans, such as the introduction of regular e-learning for all employees and tailor-made training for specific functions and persons with data protection responsibilities. The organisation must establish an audit framework and a programme to ensure that internal or external accredited auditors regularly verify compliance with the BCR. A mechanism must also be put in place to track all changes and inform BCR members and the supervisory authority. A list of BCR members must be maintained and made available to all members, who are required to inspect that list before transferring personal data across borders.

BCR are ultimately a formalisation and publication of the data protection management programme. At the same time, they are a mechanism for demonstrating accountability to regulators, business partners, customers and individuals and integrating data protection and security into the company's culture. Processors also gain an immediate competitive advantage compared to other service providers that do not have BCR. The benefits of BCR are apparent and should be considered by any multinational company with cross-border data flows.

6 Conclusions

BCR are not only a sustainable legal basis for data transfer but also a system that enables companies with approved BCR to be transparent to regulators, customers, consumers and business partners by disclosing the company's policies and procedures on how they process and secure personal data. At the same time, BCR help organisations demonstrate that they take data protection seriously and that they have adopted appropriate data management practices to ensure compliant and responsible data processing throughout the Group. By implementing BCR, organisations affirm their responsibility to comply with legal requirements, and regularly even go beyond, by implementing common standards and rights for individuals across the Group. BCR help to further improve the quality and maturity of the Group's privacy management programme by fostering a culture of internal compliance and accountability and strengthening the overall trust of individuals, customers, business partners and regulators.

Implementing BCR brings a whole range of benefits not only for the Group itself but also for the data subjects and the supervisory authorities. The effort involved in the approval and implementation process pays off in any case, measured by the advantages for multinational companies, large or small, which stand for the legally compliant and responsible handling of personal data. At the same time, and as further motivation for companies to invest in BCR, it would be desirable for supervisory authorities to formally recognise BCR as an accountability system beyond a data transfer mechanism, along with certifications and codes of conduct, and to find ways to further speed up the approval process.

Daniela Fábián Masoch

FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

Daniela is the founder and executive director of FABIAN PRIVACY LEGAL, a law firm specialised in international, European and Swiss data protection laws, governance, risk management and programme implementation. Daniela is an attorney at law and Certified Privacy Professional with over 25 years of experience in data protection, labour law, risk and programme management, security and related matters. She advises multinational companies from various industries in the EU, Switzerland and the US on the evaluation, development and implementation of data protection strategies, governance models and global privacy programmes, as well as data transfer mechanisms, with a pragmatic approach. Before commencing her own business in 2015, Daniela held various positions at Novartis, including Global Head of Data Privacy, where she was responsible for setting the Group's strategic direction for privacy, and for building, implementing and overseeing the global privacy function, global privacy management programme and Group BCR.

FABIAN PRIVACY LEGAL

FABIAN PRIVACY LEGAL is a boutique law firm specialising in international, EU and Swiss privacy laws and related matters, privacy policies, risk management and programme implementation.

Our strengths are the combination of expert knowledge and practical in-house experience, an excellent network with industry groups and data protection associations, and close cooperation with experts from a variety of related fields, such as cybersecurity and cybercrime, as well as corresponding law firms advising on local legal issues. We approach mandates with a global, solution-oriented and practical approach to deliver pragmatic and sustainable solutions.

Our clients are large and small companies in a wide range of industries, including pharmaceuticals, biotech and medical devices, technology, consumer goods, luxury goods and beverages, transportation and logistics, automotive, insurance, financial institutions and chemicals.

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
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com