This article appeared in the 2014 edition of The International Comparative Legal Guide to: Data Protection; published by Global Legal Group Ltd, London. www.iclg.co.uk

ICLG

The International Comparative Legal Guide to:

Data Protection 2014

1st Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

BANNING
Barrera, Siqueiros y Torres Landa, S.C.
CMS Reich-Rohrwig Hainz
Dittmar & Indrenius
DLA Piper
ECIJA ABOGADOS
Eversheds
Gilbert + Tobin Lawyers
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
KALO & ASSOCIATES
Koep & Partners
Marrugo Rivera & Asociados, Estudio Jurídico
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Raja, Darryl & Loh
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Account Managers
Edmond Atta, Beth Bassett, Antony Dine, Susan Glinska, Dror Levy, Maria Lopez, Florjan Osmani, Paul Regan, Gordon Sambrooks, Oliver Smith, Rory Smith

Sales Support Manager
Toni Wyatt

Sub Editors
Nicholas Catlin
Amy Hirst

Editors
Beatriz Arroyo
Gemma Bridge

Senior Editor
Suzie Kidd

Global Head of Sales
Simon Lemos

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 2014

ISBN 978-1-908070-98-2
ISSN 2054-3786

Strategic Partners

General Chapter:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides the international practitioner and in-house counsel with a comprehensive worldwide legal analysis of the laws and regulations of data protection.

It is divided into two main sections:

One general chapter entitled *Data Protection – a Key Business Risk*.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 29 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editor Bridget Treacy of Hunton & Williams for her invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.co.uk.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

Data Protection – a Key Business Risk

Hunton & Williams

Bridget Treacy

Data is the lifeblood of today's digital economy. The rapid expansion of digital commerce means that frequently data is a businesses most valuable asset. Yet the risks inherent in data, and the differing regulatory requirements around the globe, make it challenging for businesses to manage data risks in consistent, practical and cost-effective ways. Businesses that think strategically about the creation, development, use and security of their data are able to increase the value of these assets, and often enhance their reputation. Organisations that fail to take data protection compliance seriously, or fail to manage their data assets strategically, risk being left behind.

Data Protection Issues are Mainstream Issues

The exponential increase in the rate at which data is generated, together with the ready availability of cheap data storage and data processing capacity, are fuelling the growth of our digital economy. The explosion in digital commerce has had a far-reaching and permanent impact on the global economy, affecting businesses of all sizes. In 2012, over 2.3 billion people were estimated to have access to the Internet, and that number is expected to increase to 5 billion by 2020[1]. Significantly, digital commerce is not just for larger, first world economies. The availability of mobile technologies means that smaller, less developed regions can also participate.

Businesses keen to take advantage of the global digital economy, and those wishing to use data closer to home, are discovering that data protection compliance and risk management are now mainstream business issues that require careful consideration. Recent instances of data security breaches underscore the fact that global data collection and processing can give rise to global risk management issues, global PR issues, and the possibility of legal claims from multiple jurisdictions. But security breaches are not the only risk issue. There is a more recent trend of consumer complaints, sometimes by representative groups, in circumstances where consumers have felt that data collection practices are too aggressive, or data use is insufficiently transparent. Other key themes in global data protection risk management are set out below.

- Data protection is a trust issue: the general public has greater awareness of data protection rights and of the perils of poor data handling practices. Trust is broken by poor data handling procedures, including security breaches and overzealous collection and use of personal data. The costs of persuading customers to remain with a business after a security breach have been tracked by researchers for several years. One recent survey estimated that the cost of lost business accounts for more than 50% of the total cost of a data breach[2]. Elsewhere, insufficiently transparent data collection practices (for example, utilising apps installed on smart phones, or smart appliances with limited or no privacy notice) or errors in data collection (for example, Google Street View's inadvertent collection of wi-fi data) may impact consumer trust, even if laws are not violated.
- Data transfer restrictions may impact trade: many countries around the globe have imposed restrictions on cross border data transfers, and some require localised data storage. Aside from the challenges of finding workable solutions to these restrictions in practice, these restrictions can impact scalability and cost efficiency, and are becoming intertwined with the ability to trade freely, raising a new set of challenges for global businesses.
- Regulators enjoy enhanced enforcement powers, activity and cooperation: data protection authorities have gained new enforcement powers in recent years, including the power to impose fines and to audit business' compliance with data protection laws. These regulators have become proactive in bringing enforcement proceedings, and adept at using the media to publicise their enforcement actions. Further, data protection authorities increasingly seek to work collaboratively as a group, across many jurisdictions, to ensure better data protection enforcement.
- Senior executive accountability: many companies find it challenging to secure appropriate senior executive support for data protection governance initiatives. However, in certain jurisdictions senior executives can be held personally accountable for violations of data protection laws. There is precedence of enforcement action taken directly against senior executives, including prison sentences (for instance, the Italian YouTube case, although the prison sentences against three Google executives were later overturned on appeal).
- Individuals are concerned that technology is intrusive: individuals have a sense that they have lost control over their data. This has been demonstrated over recent years by public protests, complaints about the ways in which large technology companies (in particular) collect and use data, and by the growth in consumer complaints and lawsuits.

Inherent Tension Between Business Use of Data and Individual Rights

Much of the data processed within business systems is about individuals, and individuals have rights in relation to their data. There is an obvious area of friction here: businesses wish to gather and use ever increasing amounts of information about people, yet this is only permitted in compliance with laws that safeguard the rights of individuals. In Europe, the right to data protection is a fundamental right, whose history can be traced back to the post-

World War II era when secret reporting by the State about citizens was commonplace. Individuals had no right to find out whether, and, if so what, information was held about them, or to verify or correct it. Decisions were based on the content of the State's files, sometimes with tragic consequences. In 1980 the Organisation for Economic Development sought to address these issues in its Recommendations and Guidelines ("OECD Guidelines") in relation to personal data[3], and similar principles are reflected in the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention 108")[4]. The principles articulated in the OECD Guidelines and Convention 108 are reflected in the current European Data Protection Directive EC/95/46 (the "EU DP Directive")[5], giving individuals enforceable rights in relation to their data and imposing obligations on organisations that collect and process personal data.

In other jurisdictions, data protection has a different legal or historic basis. In some countries, data protection laws have evolved primarily to prohibit unwanted marketing activities, or other specific societal concerns. Almost 100 countries have passed some form of data privacy legislation, although there is considerable divergence from one country to another. There is no common position on basic concepts (such as what constitutes "personal data"), and there are overarching philosophical differences on how to restrict the collection and use of such data. Even where concepts of "privacy" and "data protection" overlap across jurisdictions, individual countries have taken different approaches to protect the data of their citizens, and strike a balance between public and private interests in this area. As a consequence, in practical terms, companies are confronted by a patchwork of data privacy laws, making compliance, or the strategic use of data, challenging.

What Data Protection Risks do Global Companies Focus On?

The data protection challenge for companies that operate on a global basis is multi-faceted. Compliance with local laws is the most basic requirement, but it is complicated by the fact that the same issue might be treated very differently under differing local laws. Where a company deploys the same technology on a global basis, it can be extremely difficult to ensure legal compliance across jurisdictions that take differing approaches to the same issue. Sometimes differences arise in relation to the most fundamental of issues – such as the meaning of "personal data". In a world in which commerce is increasingly global, even companies that operate domestically may find themselves having to address global issues where they utilise outsource vendors based off-shore, or cloud-based platforms.

In addition to legal compliance issues, businesses also focus on data as an operational risk issue. Data and IT security are generally key focus areas within this risk category. Often separate teams address these issues, although there is an emerging trend for data security and data protection leaders to collaborate on data governance and strategy.

Companies that seek to develop their data assets in more strategic ways are looking beyond mere legal compliance. For these companies, legal compliance is merely the starting point. They also pay attention to the reputational risks raised by data privacy. A security breach or the roll out of new tools or technologies that are regarded by the market place as detrimental to user privacy can have far reaching consequences for a company's reputation, and share price. Leading companies are now including data privacy risk within their ethics and governance programmes.

A growing number of companies are focusing on reticence risk. This is the risk of understanding too little about the company's own data assets, or legal framework, so that the company's approach to utilising its data assets is too conservative. The risk then is that the company misses opportunities that its competitors are only too willing to take, or simply disadvantages itself by being too conservative.

In addition to determining how the business will manage legal compliance and other heads of risk, there are several specific data privacy issues that currently challenge global businesses. These are described in more detail below.

Big Data Analytics

The term "big data" describes the collation of vast stores of data, gleaned from many disparate sources. Increasingly, it includes data that are observed, rather than created, and generally it includes personal data. Analytics are deployed to identify patterns and insights from these vast data sets and are used to learn more about consumer behaviour, to modify products or services, or to create new offerings. Businesses seeking to utilise big data need to focus on a range of data protection issues, in particular, data quality principles.

From an EU perspective, there are several important aspects of legal compliance that need to be considered in a big data context, but the key issue is the requirement that data processing must be fair and lawful, and that organisations must satisfy a legal basis for processing personal data. "Fairness" requires transparency, usually satisfied by the provision of notice. Individuals have the right to know whether their personal data are being processed and for what purpose, how the data were collected, with whom the data will be shared, and to obtain a copy of their personal data. Again, complying with these requirements can be difficult in a big data context. Where data have been collated from many sources, even the provision of notice may be a challenge. Consent and "legitimate interests" are two common legal bases to justify data processing. In a big data context, both can be difficult to satisfy. For example, where data are collated from disparate sources there may be no relationship with the individual, making consent impractical.

In addition, the purpose limitation principle provides that personal data collected for one purpose may not be used for other purposes, without the consent of the individual. However, when big data sets are collated, the purposes for which those data ultimately may be used may not yet be known.

Another issue that may raise difficulties is the data minimisation obligation. This requires that data must be relevant and not excessive for the purposes for which the data were collected. There are obvious tensions between data minimisation and big data. Restrictions on data retention mean that personal data may only be kept for as long as necessary for the purposes for which it was collected. In other words, it is not permitted to retain personal data indefinitely, yet that is what big data expects.

European data protection regulators expect companies that roll out big data programmes to focus on privacy by design, building data safeguards and compliance into the design of the big data initiative. In addition, conducting a privacy impact assessment – asking structured questions to determine the likely level of data protection compliance and risk for a product or service – prior to roll out can help pinpoint privacy risks before it is too late. Trying to fix the position after the data processing has been rolled out is expensive and may be embarrassing, or worse.

Cloud Computing

The cloud – characterised by large scale data storage and processing, delivery of software as an online service, and the leveraged connection of wireless devices to services and applications offered online – delivers systemic changes for business. But to realise this potential, businesses need to address the privacy questions that this technology raises, including what data protection and privacy laws apply to data that is stored in the cloud and whether data that is stored in the cloud is "transferred" internationally, so that cross border data transfer restrictions apply. Cloud computing contemplates the processing of data anywhere and everywhere, across multiple jurisdictions, simultaneously, whereas while most data protection laws and guidance anticipate linear transfers of information from point A to point B. Traditional approaches to cross border data transfers, such as Model Clauses or the EU/U.S. Safe Harbor, may not offer a workable solution in the cloud context, or may be cumbersome to implement and maintain.

A second issue that usually arises when companies consider the cloud is the issue of security. Companies must ensure adequate security for the storage and processing of their personal data, whether they venture into the cloud or maintain physical, local processing centres. Companies using cloud computing models must be able to adequately reassure individuals that their data will be safeguarded. Security concerns may be magnified by the dynamic nature of the cloud environment, but can also be more robust than in the physical world.

Perhaps the greatest cloud risk of all is connected to the fact that cloud-based processing is often inexpensive. Frequently, organisations are not even aware that their data are processed in the cloud, as the cost of processing may fall below internal spending approval thresholds.

Internet of Things

The phrase "Internet of Things" (or "IoT") was first used to describe the difference between data created by humans and data created by "things". It was predicted that, as the Internet evolved, "things" would increasingly create data on their own, without the need for direct human input. IoT now refers to a network in which machines produce and share data automatically in response to events, without requiring human involvement. However, it is difficult to define IoT precisely because the technology and its applications change constantly. Examples of IoT include: household smart meters (which measure and adapt to an individual's use of utilities); smart phones that routinely collect data, such as health data, that can be shared with healthcare apps and services; and trainers and fitness bracelets that collect information about running style and exercise patterns.

There is tension between the efficiency and convenience that IoT offers and the risk that IoT devices will invade formerly private spaces and share data that would not otherwise have been available. Smart meters provide an example of this tension; they can help to reduce energy use and cost, but they can also reveal large amounts of personal household information to an energy provider. The privacy challenge for companies is to determine what is the right balance between giving consumers the services they want, and ensuring that their privacy is respected. In most cases, users are happy to agree to standard terms and conditions to receive a free service. But once data leaks onto the Internet, it is almost impossible to delete it. Further, the risk of unforeseen consequences is significant, as previously separate pools of data are more frequently combined in the IoT context.

The evolving nature of IoT means that there can be an uneasy fit with laws that were drafted before this technology existed. For example, how can meaningful consent be obtained from users of smart devices. How can a smart device can provide users with notice of the purposes for which their data will be processed? Given the lack of certainty in this area, companies seeking to be part of the IoT would be well advised to conduct thorough privacy impact assessments before rolling out new products.

Cross Border Data Transfers and Interoperability

Many data privacy laws prohibit or restrict the international transfer of personal data. Consent or limited derogations may enable certain transfers to take place, but the future of global commerce demands data transfer mechanisms that are flexible and able to accommodate appropriate, large-scale data transfers. Some regimes waive general data transfer restrictions where transfers are made to specific, pre-approved jurisdictions. For example, in the EU, personal data may be transferred freely to countries deemed by the European Commission to have "adequate" data protection laws in place, or where pre-approved mechanisms (such as Binding Corporate Rules, Safe Harbor or EU Model Clauses) are used. In the UK, organisations can make their own adequacy assessment when transferring personal data abroad, determining whether the level of data protection available is adequate in all the circumstances.

The challenges associated with complying with cross border data transfer restrictions are not new issues, but there remain surprisingly few accepted transfer mechanisms. Those that are available often are complex or even unworkable where transfers are made to multiple entities in multiple jurisdictions. Model clauses can be particularly bureaucratic to implement and maintain. Recent adoption of the APEC region's Cross Border Privacy Rules[6], and close analysis of them by European data protection authorities, has raised renewed interest in the possibility of creating an interoperable approach to cross border data transfers that satisfies regional data protection laws. Other mechanisms are also under discussion, including a European data protection seal programme that would permit certified organisations to transfer to and receive personal data from other certified organisations, irrespective of their location.

The Role of Accountability

Accountability is a term that has been used more frequently in a privacy context during the last five years. It requires that businesses actively take ownership of the need to manage their information, irrespective of where it resides or is processed. Accountability is not a substitute for data protection or privacy law. An accountable organisation complies fully with applicable laws and regulation governing the collection and processing of data, but goes further, putting in place information management and privacy practices that enhance the business' brand, reputation and relationship with its customers.

This concept is not new, although its application in a privacy context is. The OECD Guidelines include an accountability principle, making organisations accountable for complying with measures that give effect to the rest of the guidance. The APEC Framework[7] articulates the accountability principle more explicitly than the OECD Guidelines. The Canadian privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA)[8] includes accountability as its first principle. A similar concept underpins the European Commission's Binding Corporate Rules mechanism governing the international transfer of European

personal data within a multinational corporate group. Yet while accountability is a well-established principle of data protection law, little has been written to describe what an organisation must do to be accountable, or how an accountability mechanism might resolve jurisdictional and local law issues.

Legislative Change: European Commission's Proposal for Data Protection Regulation

On January 25, 2012, the European Commission released its data protection law reform package. Two new pieces of EU law, a general data protection regulation (the "Regulation")[9] and a directive on processing for crime and criminal justice purposes (the "Directive")[10], will repeal and replace the current EU DP Directive and Framework decision 2008/977/JHA on data protection in police and judicial cooperation in criminal matters. The proposed Regulation will likely have most impact on commercial organisations.

The legislative process has become stalled given the approaching European elections in May 2014, but the European Parliament has voted to adopt an amended draft of the Commission's proposal, signalling the likelihood that the proposal will be progressed under the next Parliament. At the time of writing, the Council's position on the draft text is still under negotiation. Once an agreed position is reached, a trilogue involving the Commission, the Parliament and the Council will commence. The timing of any such discussions or, indeed on reaching agreement on the text, is by no means clear. Optimists are focusing on December 2014 or early 2015. What is reasonably clear, however, is that an implementation period of approximately two years is likely.

Although the status of the legislative process is uncertain, a number of key issues raised by the Commission's draft Regulation would bring far-reaching changes for companies doing business in Europe. Some of the key proposals are described briefly below.

Harmonisation

The EU DP Directive required local implementation by each Member State. As a consequence, there is a patchwork of 28 separate data protection laws within the EU, each of which must be complied with by organisations operating in multiple jurisdictions. In contrast, the Regulation would take direct effect in every Member State without any need for local implementing law. This would streamline and harmonise EU data protection law, but local variances will still remain in some areas, such as processing for health, employment and statistical purposes.

One Stop Shop and Consistency Mechanism

The term "one stop shop" was coined to describe a solution to one of the more frustrating aspects of the current regime: at present, organisations may be subject to the supervisory powers of the data protection authorities of several Member States, each of whom may have a different approach to an issue and differing powers of enforcement. For organisations, it is time consuming to deal with multiple regulators, and difficult (and expensive) to accommodate the differing approaches that regulators may take in relation to the same issue. The Commission's proposal is that only one regulator, the lead supervisory authority, would take decisions against the organisation. Where an entity has operations in several Member States, the lead supervisory authority will be that of the jurisdiction in which the "main establishment" of the company is located.

Associated with this is the consistency mechanism, which refers to a decision-making process that promotes consistent decisions across Member States. In the Commission's proposal, where a case does not have EU-wide impact, the relevant national regulator would make its own decision, without consultation. If the issue had an EU impact, it would be considered by the EU Data Protection Board, which could issue an opinion which the national regulator would need to take into account. This formulation envisaged the Commission acting as a back stop, with the ability to make a non-binding intervention or to require the national regulator to take certain steps. The Commission's formulation is not universally accepted, however, and particular difficulties stem from the mechanics of how the one stop shop regime will work in practice where the laws of other Member States, in which the main establishment is not located, continue to apply.

Extra-Territorial Effect

The EU DP Directive applies to organisations established within the EU or that make use of data processing equipment situated within the EU. The Regulation would apply to organisations established in the EU, and also to some organisations established outside of the EU who offer goods or services to data subjects in the EU or monitor the behaviour of data subjects in the EU. This will mean that many non-EU businesses, particularly those active online, will find themselves subject to European law.

Breach Notification Requirements

The Regulation would introduce stringent data breach notification requirements that would apply across all sectors. Breaches would need to be reported to the supervisory authority within a specified timeframe – likely 72 hours. Where the breach is likely to affect the privacy of individuals, affected data subjects must also be notified.

Accountability

Regulation introduces a number of requirements designed to make organisations more accountable in their data processing activities. Organisations will be obliged to process data in accordance with the provisions of the Regulation; to demonstrate compliance; create and retain documentation on data processing activities; design processing with inbuilt privacy protections; and appoint data protection officers. The criteria for the appointment of a data protection officer are not yet agreed, but there may be an exemption for smaller organisations, or those that process limited amounts of personal data.

Enforcement

Enforcement powers under the EU DP Directive are fractured and disparate. Under the Regulation, all supervisory authorities will be able to enforce monetary penalties. The level of monetary penalties is not yet settled, but may be as high as 5% of global turnover.

Strengthening of Data Subject Rights

The Regulation strengthens the rights of data subjects and shifts the burden of establishing such rights away from individuals and towards organisations processing their personal data. The pre-existing right of erasure is bolstered by an explicit "right to be forgotten", obliging organisations not only to delete data but to delete links to, or copies of, data that are under their control and to inform recipients of the data that the individual requires to be

deleted. Individuals will also have a new express right of data portability, greater informational rights (including to be informed on collection of retention periods, potential third party recipients and the right to complain to supervisory authorities) and a general right to not be subject to automatic profiling.

Future of Data Protection

Data assets will remain critical to future business success, so data protection compliance and governance will become critical risks for businesses to understand and address. Companies that succeed will be those that anticipate data uses, secure their data assets and understand the risks inherent in their data. Companies that do not focus on personal data will miss opportunities, or face compliance issues.

Endnotes

1 International Telecommunication Union, Measuring the Information Society 6-7 (2012), available at http://www.itu.int/pub/ D-IND-ICTOI-2012/en (last visited April 2, 2014).

2 Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, p. 18, Figure 19, Percentage of lost business costs relative to total average cost, 2013 figures for the U.S., available at http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf (last visited April 2, 2014).

3 The OECD Privacy Guidelines, last revised 2013, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (last visited April 2, 2014).

4 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.1.1981, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (last visited April 2, 2014).

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited April 2, 2014).

6 APEC Cross-Border Privacy Rules System, available at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx (last visited April 2, 2014).

7 APEC Privacy Framework, December 2005, available at http://publications.apec.org/publication-detail.php?pub_id=390 (last visited April 2, 2014).

8 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, available at http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-1(last visited April 2, 2014).

9 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (last visited April 2, 2014).

10 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:HTML (last visited April 2, 2014).

Bridget Treacy

Hunton & Williams
30 St Mary Axe
London, EC3A 8EP
United Kingdom

Tel: +44 207 220 5700
Fax: +44 207 220 5772
Email: btreacy@hunton.com
URL: www.hunton.com

Bridget Treacy leads Hunton & Williams' UK Privacy and Cybersecurity team and is also the Managing Partner of the Firm's London office. Her practice focuses on all aspects of privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget's background in complex technology transactions enable her to advise on the specific data protection and information governance issues that occur in a commercial context. Bridget is the editor of the specialist privacy journal "Privacy and Data Protection", and has contributed to a number of published texts. According to Chambers UK, "She is stellar, one of the leading thinkers on data protection, providing practical solutions to thorny legal issues".

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 and 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
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet

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