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 978-1-910083-45-1
ISSN 2054-3786

Strategic Partners

General Chapter:

1	**Legislative Change: Assessing the European Commission's Proposal for a Data Protection Regulation** – Bridget Treacy, Hunton & Williams		1

Country Question and Answer Chapters:

2	**Australia**	Gilbert + Tobin: Peter Leonard & Michael Burnett	7
3	**Austria**	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	17
4	**Belgium**	Hunton & Williams: Wim Nauwelaerts & David Dumont	28
5	**Brazil**	Opice Blum, Bruno, Abrusio & Vainzof Advogados Associados: Renato Opice Blum & Renato Leite Monteiro	36
6	**Canada**	Osler, Hoskin & Harcourt LLP: Adam Kardash & Bridget McIlveen	45
7	**China**	Hunton & Williams LLP Beijing Representative Office: Manuel E. Maisog & Zhang Wei	54
8	**Cyprus**	A.G. Erotocritou LLC: Alexis Erotocritou	60
9	**Finland**	Dittmar & Indrenius: Jukka Lång & Iiris Keino	68
10	**France**	Hunton & Williams: Claire François	76
11	**Germany**	Hunton & Williams: Dr. Jörg Hladjk	84
12	**India**	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	95
13	**Ireland**	Matheson: John O'Connor & Anne-Marie Bohan	106
14	**Italy**	Portolano Cavallo Studio Legale: Laura Liguori & Federica De Santis	117
15	**Japan**	Mori Hamada & Matsumoto: Akira Marumo & Hiromi Hayashi	125
16	**Lithuania**	Juridicon Law Firm: Laimonas Marcinkevicius	135
17	**Luxembourg**	Jurisconsul: Erwin Sotiri	142
18	**Mexico**	Hogan Lovells BSTL, S.C.: Mario Jorge Yanez V. & Federico de Noriega O.	150
19	**Netherlands**	Brinkhof: Quinten Kroes & Tineke van de Bunt	158
20	**New Zealand**	Wigley & Company: Michael Wigley	169
21	**Norway**	Wikborg, Rein & Co. Advokatfirma DA: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck	175
22	**Portugal**	Cuatrecasas, Gonçalves Pereira: Leonor Chastre	185
23	**Puerto Rico**	Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.: Alejandro H. Mercado & Shylene De Jesús	195
24	**Romania**	Pachiu & Associates: Mihaela Cracea & Ioana Iovanesc	201
25	**Russia**	Gorodissky & Partners: Sergey Medvedev Ph.D., LL.M.	211
26	**South Africa**	Eversheds: Tanya Waksman	221
27	**Spain**	ECIJA ABOGADOS: Carlos Pérez Sanz & Lorena Gallego-Nicasio	228
28	**Sweden**	Affärsadvokaterna i Sverige AB: Mattias Lindberg	237
29	**Switzerland**	Pestalozzi: Clara-Ann Gordon & Dr. Michael Reinle	245
30	**Taiwan**	Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Rebecca Hsiao	254
31	**Turkey**	ELIG, Attorneys-at-Law: Gönenç Gürkaynak & İlay Yılmaz	262
32	**United Kingdom**	Hunton & Williams: Bridget Treacy & Anita Bapat	271
33	**USA**	Hunton & Williams LLP: Aaron P. Simpson & Chris D. Hydak	279

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

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

Hunton & Williams

Bridget Treacy

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

After protracted negotiations lasting more than three years, it now seems that Europe's data protection reforms will result in new legislation. At the time of writing, there is a palpable sense of purpose in Brussels surrounding the progress of the Proposed General Data Protection Regulation, with optimists suggesting the law may be finalised by the end of 2015 or early 2016. A two year implementation period is anticipated. On close reading, it is apparent that many of the proposals are largely agreed. Organisations should now be thinking carefully about their preparation for Europe's new data protection regulation, not least because of the significant fines (of as much as 5% of annual global turnover) and sanctions that seem likely to be part of the reform.

Status of European Legislative Reform

The European Commission released its data protection law reform package on 25 January 2012. Two new pieces of EU law, a general data protection regulation (the "Regulation") and a directive on the processing of personal data by competent authorities for criminal justice purposes (the "Directive"), will repeal and replace the current EU Data Protection Directive and Council Framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The discussion in this paper focuses only on the Regulation.

The European Commission's text was presented to the European Parliament and the Council of Ministers at the same time. The European Parliament considered several thousand amendments and adopted an agreed amended text just prior to the end of the Parliamentary term in March 2014. Broadly speaking, the Parliament sees itself as the champion of the individual, and many of its proposals can be seen to strengthen the rights of individuals, and impose further constraints on data processing by organisations.

The process now awaits a proposal from the Council of Ministers, which represents the Member States' governments. The Council's amendments reflect the interests of governments and, to some extent, the business community. The work on behalf of the Council has been led by the DAPIX Working Group which has adopted a partial, general approach. As discussions have progressed, the Working Group has published sections of text, complete with reservations maintained by Member States, on the basis that nothing is agreed until the whole text is agreed. Once finalised, the text must be agreed by the Council of Ministers. It is not known when the final proposed text will be sent to the Council. This might still occur before June 2015, when the Latvian Presidency ends. The Council Presidency then rotates to Luxembourg for the latter half of 2015.

Once the Council's text is adopted, the Council, European Commission and European Parliament will engage in a trilogue and seek to reach agreement on a final legislative text. Optimists have predicted that the trilogue will take only six months to reach agreement. The more widely held view is that agreement will not be achieved until the first half of 2016. A two year implementation period is then expected. Despite uncertainty about the timing of the process, what is now clear is that the proposal is likely to result in new legislation. It is therefore timely to stand back and consider some of the key themes that are emerging from the respective texts, and how companies should now be preparing for the changes that lie ahead.

Key Themes

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 existing European Data Protection Directive required local implementation by each Member State. As a consequence, there is a patchwork of 28 separate data protection laws within the EU, and organisations that operate in multiple Member States must comply with differing laws across 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, although local variances will still remain in some areas, such as processing personal data 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 which 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 would 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 a yet to be established EU Data Protection Board, which could issue an opinion which the national regulator would need to take into account. This formulation envisages 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 has been widely contested, however. 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. As matters stand, this is one of the most significant issues that must still be agreed.

Extra-Territorial Effect

The EU Data Protection Directive applies to organisations that are established within the EU, or 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 that offer goods or services to data subjects in the EU or monitor the behaviour of data subjects in the EU. This would mean that many non-EU businesses, particularly those active online, will find themselves subject to European law.

Breach Notification Requirements

The Regulation seems certain to 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

The 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; be prepared 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 Data Protection Directive vary considerably. 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 annual 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 the organisations that process their personal data. The 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.

Comparing and Contrasting the Approaches of the Parliament and the Council

As the legislative process moves towards a trilogue, it is useful for organisations to consider how the approaches of the Parliament and the Council differ, and where there is common ground.

Parliament's Proposal

Unsurprisingly, the Parliament's text tends to favour the individual, strengthening the position of data subjects, and increasing the compliance obligations of data controllers. These proposals are not necessarily bad for business. The Parliament's approach introduces some practical and pragmatic changes, including the very welcome extension of the One Stop Shop concept to groups of undertakings (rather than being limited to a single undertaking, as proposed by the Commission), requiring agreements between joint controllers to allocate tasks associated with data subjects between the parties, developing the concepts of data protection seals and certifications, restricting the circumstances in which controllers must apply for prior approval, and generally reducing the amount of paperwork prescribed for controllers.

Stronger Rights for Individuals

On the theme of stronger rights, the Parliament's text extends the notice and transparency provisions proposed by the Commission. In particular, the proposed Article 13 requires standardised privacy policies and introduces a series of icons to enable individuals to see, at a glance, how their information will be processed. The notice and transparency provisions are wider than those in the Commission's draft. In particular, the information to be provided to individuals would be more detailed. These requirements would probably be difficult to accommodate within existing notices and could require changes to the way that notices are provided.

The Parliament text proposes an absolute right to object to processing carried out on the basis of the controller's legitimate interests, and restricts the use of data for new and incompatible purposes. The Commission's text provided that legitimate interests cannot be used as a basis to justify the use of personal data for new purposes that are incompatible with the purpose for which the data were collected. The Parliament's text removes this provision, apparently with the intention that data cannot be used for a new and incompatible

purpose without some form of prior authorisation by the data subject such as notice and consent.

Increased Controller Obligations

For controllers, an example of more stringent obligations includes the significant extension of the sensitive data category so that only the most general information would be non-sensitive. The category would include gender identity, and details of administrative sanctions, judgments, and criminal or suspected offences. These categories of data could only be processed under the control of an official authority or when necessary for limited reasons e.g. compliance with a legal obligation.

Other examples of more stringent obligations include the requirement that consent be purpose specific and lose its validity once the relevant purpose ceases to exist, the inclusion of overseas controllers within the scope of the Regulation, the tightening of exemptions, and a proposal to increase the maximum fine to 5% of annual global turnover.

Council's Proposal

As has been explained, the Council text has not yet been agreed, and its final views are not known. Currently, the Council is debating the role of supervisory authorities, cooperative working and the One Stop Shop proposal. It has also sought to reduce the administrative burdens on businesses from those proposed in the Commission's text, and it has introduced the concept of proportionality in responding to compliance challenges.

One Stop Shop

On the important issue of cooperative working between supervisory authorities and One Stop Shop, the Council is focused on local resolution of complaints and directing individual complaints to the supervisory authority for the jurisdiction in which the data subject resides. It has also sought to distinguish investigatory, corrective and authorisation powers. Perhaps controversially, it proposes that the European Data Protection Board is established as an institution of the European Union.

Reducing Administrative Burdens

In seeking to reduce administrative burdens on controllers and processors, the Council text does not include requirements for generalised policies. The subject information provisions are less detailed and less prescriptive than those proposed by the Parliament, and similar to those required by the current Data Protection Directive, differentiating between those provided directly to the individual and those provided where the information is obtained from a third party. Where there is an obligation to have policies, this seeks to be proportionate. Record keeping requirements do not apply where the processing is low risk and does not involve specific risks to the rights and freedoms of individuals.

Risk Based Approach

In introducing a risk based approach, the Council makes increased provision for exemptions and makes the right to object to data processing more restrictive. Data breach reporting, for example, would only be required for breaches that have a serious impact, and steps taken after the breach to mitigate risk may be taken into account in deciding whether to notify. The text delineates the roles of controller and processor more clearly.

Areas of Agreement, and Disagreement

There remain significant differences between the three texts, and resolving those differences will not be easy. Now, more than ever, organisations need to stay engaged with the process, and remain vigilant. Apparently small changes to the text can have a significant impact, and may greatly increase the compliance burden. With this in mind, this section will explore where there has been a growth in consensus around new, emerging issues, and where there is a substantial degree of commonality despite small textual differences. The section will also identify the areas where there are clear and specific disagreements that will no doubt be the subject of further negotiation.

Common Themes

It is not an exact science to identify common themes as there remain many textual differences, but some are emerging. The first to note is that there appears to be general support for the development of seals, certifications and codes of conduct. These are particularly evident in the Council's draft text as part of its broader risk-based approach, but the tools feature strongly in the other texts as a means of enabling strong data protection.

There appears to be some commonality on the development of factors that will aid good decision-making, such as the selection of a main establishment, and the issues that are relevant to determining sanctions. There also seems to be partial agreement as to the nature and role of the EU Data Protection Board. Although this raises political issues, particularly for the UK (which opposes the creation of a new EU institution) the Commission's original proposal envisaged a strong role for the Commission which has been largely replaced by the EU Data Protection Board. Even if the EU Data Protection Board does not become an institution of the European Union with legal personality and powers, it seems likely to take on many of the tasks that originally were allocated to the Commission. This appears to have been accepted by all the parties, and is a welcome development.

Limited Variation

In addition to common themes, there are a number of areas in which there are only limited variations between the texts. These include the need to appoint a data protection officer (and the nature of that role), the role and powers of supervisory authorities (excluding discussions of the One Stop Shop), the data protection principles themselves, rights to subject access, data portability and rectification, and the need for contracts between controllers and processors to specify their responsibilities for data protection. There remains some variation between the draft texts on these issues but the core position is not radically different between the texts, and it is to be hoped that differences can be resolved without too much difficulty.

Significant Variation

There remain a number of areas in which there remain key differences in the detailed text.

Definitions

There remains a lack of agreement over significant definitions (apart from the definitions of processing, filing system, controller and processor). Other definitions still under consideration are those relating to personal data, profiling, consent, genetic data, main establishment and pseudonymous (data), all of which may impact the potential reach of the law. In addition, the amendments to the definition of binding corporate rules ("BCRs") in the Council text would mean that BCRs could apply as between "groups of enterprises engaged in joint economic activity", which would greatly widen the scope of BCRs.

Breach Reporting

Under the Commission proposal there is no harm threshold for notification of data breaches to the supervisory authority and notice is required within 24 hours, if possible. The Parliament removed the 24 hour timeframe and the Council went further so that notification is only required where the breach is "likely to severely affect the rights and freedoms of data subjects". None of the texts require notice to the data subject if the data are encrypted, but the Council would also remove the obligation to notify data subjects where the controller has taken subsequent measures (even after the breach) to ensure that data subjects' interests are safeguarded. Although there seems to be agreement that breach reporting will be required, there is no agreement as to what will trigger the need to report.

Sanctions

The sanctions are essentially the same across all three texts, but the level of fines differs significantly. The Commission text proposed a maximum fine of 2% of annual global turnover; Parliament raised this to a maximum of 5%. The Council has not yet stated its view. Under the Parliament text, if a controller or processor has a seal, then there would be a fine only for intentional or negligent breach. The Parliament text would also formalise the considerations that should be taken into account in determining the sanction, such as the nature and gravity of the offence, the data affected, the level of damage caused, and steps taken to mitigate the impact. Penalties (i.e., criminal sanctions) may be imposed by Member States for breaches as well as administrative fines.

Overseas Transfers

One of the stated aims of the review of the Data Protection Directive was to make the process for transferring personal data outside the EU more straightforward. The Commission text, the Parliament text and the Council text follow the same mechanisms for transfer (i.e., adequacy decisions, approved contractual clauses, BCRs, and derogations) but there are significant differences between the ways in which these mechanisms would apply. Under the Parliament text existing findings of adequacy and decisions on standard contractual clauses would expire five years after the introduction of the Regulation, unless replaced in that time. Under the Parliament text, BCRs would not be available for data processors but could be extended to sub-contractors of a data controller.

The Parliament text recognises the possibility of adequate protection being based on the application of a "European Data Protection Seal". The Council has adopted a similar concept with transfers being potentially acceptable subject to an approved code of conduct or an approved certification mechanism. The Parliament text would not allow transfers on the basis of legitimate interest.

The Parliament text also restricts the transfer or disclosure of personal data to overseas authorities in a new Article 43a. This appears to be directly aimed at U.S. authorities that seek to obtain data on EU citizens. Such requests must be referred to the supervisory authority.

Where the Texts are Unclear

In the areas just discussed, the areas of divergence are reasonably clear. There are, in addition, a number of areas in which the final position is far from clear, and some of these areas are key. An example is consent. The Commission and the Parliament text define consent as requiring an "explicit" indication. The Council has removed this from the definition but has added the concept of "unambiguous" consent for most data. Unambiguous consent could be implicit but must be clear. Explicit consent will remain the standard for sensitive personal data. The Commission has proposed that consent would not offer a legal basis for processing where there is a "significant imbalance" between data subject and controller. In addition, the Parliament text proposes that consent is purpose limited and that it will lose its validity when the relevant purpose is achieved. The Parliament has also proposed that consent to the use of data for another purpose cannot be made a condition of a contract. Clearly there remains a divergence of views on this fundamental issue.

Differences also exist on the requirements for data protection impact assessments, prior authorisation and lifecycle risk assessments. The Parliament text has extended the entire risk assessment process and added two new Articles, 32a and 33a. These Articles only appear in the Parliament text and may therefore be vulnerable to removal at the negotiating stage. Article 32a requires a risk assessment in every case of new processing to decide whether a representative should be appointed (where the controller is an overseas company that does not otherwise have to appoint one). The Parliament text lists specific categories of processing that "are likely" to give rise to specific risks. Some of these are the same as the risks identified by the Commission, but the Parliament's list of situations in which the initial risk-assessment must be conducted is extensive.

The need for a Data Protection Impact Assessment is covered in the revised Article 33, re-named as lifecycle data protection management. The Data Protection Impact Assessment must address the entire lifecycle of the data, assessing the nature of the processing and the nature of the data recipients. A new Article 33a requires a compliance review of the processing two years after the first Data Protection Impact Assessment and every two years thereafter to ensure that the processing remains compliant and is carried out in accordance with the results of the first assessment.

In contrast, the Council has limited the categories of processing regarded as risky to four: profiling causing legal effects or severe effects; sensitive data used for decisions about individuals made on a large scale; large scale monitoring of public spaces or use of genetic or biometric data; plus processing that is subject to prior consultation.

Finally, another key area of divergence relates to the One Stop Shop, discussed above. This issue is a current focus for the Council's negotiations.

What Should Organisations Do Now to Prepare?

Although some of the details remain to be resolved, there is more agreement than difference between the proposals of the Commission, the Parliament and the Council, and the direction of travel on most issues is clear. In light of this, organisations should already be taking stock of their data assets and considering how compliant their data processing activities are. Boards of Directors, CEOs and General Counsel have started to realise that irresponsible uses of data, and data breaches, can jeopardise customer trust, destroy reputations,

affect their share price, and lead to fines. These incidents can even result in senior executives losing their jobs.

Appointing a Data Protection Officer (DPO)

DPOs play a key role in managing data privacy risk. As companies search for new ways to understand their customers, manage their businesses and monetise their data assets, a DPO can help to realise these opportunities, ensuring that existing data assets are safeguarded and helping to enhance and protect a corporate reputation. Under the proposed Regulation, the appointment of a DPO will be mandatory for many organisations, recognising the key role these individuals often play.

The detailed responsibilities of a DPO will vary from one company to another, but the key focus of the role is to oversee data privacy compliance and manage data protection risk for the organisation. This is not just about legal compliance with data privacy laws and breach prevention. A DPO can actually help companies assess new business opportunities that utilise data assets.

Privacy Compliance Programme

Typically, a DPO will be responsible for creating and implementing a privacy compliance programme. This should focus on four key areas:

- legal compliance risk – ensuring that the company complies with data privacy laws wherever it does business;
- reputation risk – managing the risk of harm to a company's reputation that can arise from data protection mistakes;
- investment risk – ensuring that data privacy and security requirements are addressed early in the development of new technologies, services and processes. This can prevent disruption and additional costs to business, and limit privacy risk for both the organisation and individuals; and
- reticence risk – companies need to use data protection as a 'business enabler'. Unless companies understand and proactively address data privacy, they may overlook business opportunities, or fall behind their competitors.

Key Tools for Managing Privacy Risk

The DPO typically will utilise the following tools to implement and manage a data protection compliance programme: policies and processes; people; and technology.

Policies and processes are the rule book that describe the company's approach to data protection, and set out the guidelines and rules that staff are expected to follow. Processes include specific tools that help the company, and the DPO, to identify and calibrate privacy risk.

People are key to implementing the company's data privacy rule book. Training and awareness-raising are essential to embedding a privacy programme and building a corporate privacy culture. Staff need to know what the baseline legal requirements are, what the company's approach is, and why the company thinks data protection is important. The DPO plays a key role in raising awareness and rolling out training.

Technology refers to systems and automated controls. The DPO needs to work with the company's IT and Information Security functions to ensure that systems operate in a privacy compliant way, and that data security is ensured.

As European data protection law is reformed, existing legal requirements look set to be tightened, and sanctions strengthened. Fines of between 2% and 5% of global turnover are likely to be available under the new regime. Now, more than ever, companies need to manage data privacy risk proactively, and to remain involved in discussions about European data protection reform.

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

Tel: *+44 207 220 5700*
Fax: *+44 207 2207 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 enables 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
- 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