



ICLG

The International Comparative Legal Guide to: **Data Protection 2016**

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB

Bagus Enrico & Partners

Cuatrecasas, Gonçalves Pereira

Deloitte Albania Sh.p.k.

Dittmar & Indrenius

ECIJA ABOGADOS

Eversheds SA

Gilbert + Tobin

GRATA International Law Firm

Hamdan AlShamsi Lawyers & Legal Consultants

Herbst Kinsky Rechtsanwälte GmbH

Hogan Lovells BSTL, S.C.

Hunton & Williams

Lee and Li, Attorneys-at-Law

Matheson

Mori Hamada & Matsumoto

Osler, Hoskin & Harcourt LLP

Pachiu & Associates

Pestalozzi

Rossi Asociados

Subramaniam & Associates (SNA)

Wigley & Company

Wikborg, Rein & Co. Advokatfirma DA



Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

Copyright © 2016
Global Legal Group Ltd.
All rights reserved
No photocopying

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

Strategic Partners



General Chapter:

1	Preparing for Change: Europe's Data Protection Reforms Now a Reality – Bridget Treacy, Hunton & Williams	1
---	--	---

Country Question and Answer Chapters:

2	Albania	Deloitte Albania Sh.p.k.: Sabina Lalaj & Ened Topi	7
3	Australia	Gilbert + Tobin: Peter Leonard & Althea Carbon	15
4	Austria	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	30
5	Belgium	Hunton & Williams: Wim Nauwelaerts & David Dumont	41
6	Canada	Osler, Hoskin & Harcourt LLP: Adam Kardash & Bridget McIlveen	50
7	Chile	Rossi Asociados: Claudia Rossi	60
8	China	Hunton & Williams: Manuel E. Maisog & Judy Li	67
9	Finland	Dittmar & Indrenius: Jukka Lång & Iris Keino	74
10	France	Hunton & Williams: Claire François	83
11	Germany	Hunton & Williams: Anna Pateraki	92
12	India	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	104
13	Indonesia	Bagus Enrico & Partners: Enrico Iskandar & Bimo Harimahesa	116
14	Ireland	Matheson: Anne-Marie Bohan & Andreas Carney	123
15	Japan	Mori Hamada & Matsumoto: Akira Marumo & Hiromi Hayashi	135
16	Kazakhstan	GRATA International Law Firm: Leila Makhmetova & Saule Akhmetova	146
17	Mexico	Hogan Lovells BSTL, S.C.: Mario Jorge Yáñez V. & Federico de Noriega Olea	155
18	New Zealand	Wigley & Company: Michael Wigley	164
19	Norway	Wikborg, Rein & Co. Advokatfirma DA: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck	171
20	Portugal	Cuatrecasas, Gonçalves Pereira: Leonor Chastre	182
21	Romania	Pachiu & Associates: Mihaela Cracea & Ioana Iovanesc	193
22	Russia	GRATA International Law Firm: Yana Dianova, LL.M.	204
23	South Africa	Eversheds SA: Tanya Waksman	217
24	Spain	ECIJA ABOGADOS: Carlos Pérez Sanz & Lorena Gallego-Nicasio Peláez	225
25	Sweden	Affärsadvokaterna i Sverige AB: Mattias Lindberg	235
26	Switzerland	Pestalozzi: Clara-Ann Gordon & Phillip Schmidt	244
27	Taiwan	Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Rebecca Hsiao	254
28	United Arab Emirates	Hamdan AlShamsi Lawyers & Legal Consultants: Dr. Ghandy Abuhawash	263
29	United Kingdom	Hunton & Williams: Bridget Treacy & Stephanie Iyayi	271
30	USA	Hunton & Williams: Aaron P. Simpson & Chris D. Hydak	280

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

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication. This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Preparing for Change: Europe's Data Protection Reforms Now a Reality

Hunton & Williams

Bridget Treacy



Introduction

Europe's data protection laws are about to change. The General Data Protection Regulation ("Regulation") [1] will significantly increase the compliance obligations of organisations that process personal data, strengthen the rights of individuals in relation to their data, and extend the enforcement powers of regulators, including the ability to impose fines of up to €20 million or 4% of global revenue. The Regulation is expected to take effect in early 2018, but organisations should be assessing their compliance posture now, and taking steps to prepare for implementation. A number of changes will require a lengthy lead time to implement. This chapter offers a practical perspective for organisations preparing for change.

European Data Protection Reform

The current reform of Europe's data protection laws was prompted by a widely held view that the Data Protection Directive (EC/95/46) is out of date and no longer fit for purpose. Data processing activities are becoming ever more complex, sophisticated and ubiquitous, and the legislative framework has not kept pace with the data revolution. However, the process of reforming Europe's data protection laws has not been easy. The European Commission released its data protection law reform package on 25 January 2012. Two new pieces of EU law, the Regulation and a directive on the processing of personal data by competent authorities for criminal justice purposes (the "Directive"), were proposed, repealing and replacing 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 [2]. Political agreement on the legislative text was reached nearly four years later, on 15 December 2015. The Regulation is expected to be formally adopted during the first half of 2016, and will be followed by a two-year implementation period, coming into force in 2018.

Overview of Key Provisions

The Regulation should be regarded as an enhanced, more rigorous version of the existing Data Protection Directive and, given the hefty sanctions for failure to comply, it needs to be taken seriously. Some provisions are new, but many existing concepts have been tweaked or strengthened. Even where apparently small tweaks have been made, organisations should be cautious: in many cases, small

tweaks (such as the strengthened requirements for consent) will have a big impact on internal processes, and may take some time to embed. A number of key provisions are explained below.

Harmonisation

The existing European Data Protection Directive has required local implementation by each Member State, and individual Member States have taken differing approaches to this. As a consequence, there is a patchwork of 28 separate data protection laws within the EU, so that organisations that operate in multiple Member States must comply with differing laws across multiple jurisdictions, at considerable cost. In contrast, the Regulation will take direct effect in every Member State without any need for local implementing law. This will streamline and harmonise EU data protection law to a significant extent. Local variances will still remain in a number of areas, such as processing personal data for health, employment and statistical purposes. Additionally, Member States may decide to impose further obligations under national law.

One Stop Shop and Consistency Mechanism

The term "One Stop Shop" was originally used by the European Commission to describe a proposed solution to one of the more frustrating aspects of the current data protection 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 with business operations in several Member States, 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. Despite the European Commission's original intentions, the original "One Stop Shop" proposal has been significantly modified and diluted during negotiations to take into account technical legal concerns on jurisdiction. The supervisory authority of a business' main establishment (i.e., the place where the main processing activities take place), or its only establishment in Europe, will be the 'lead' authority for cross-border data processing [3]. In other words, if a business has multiple subsidiaries across the EU, the "One Stop Shop" is unlikely to apply, but if a single company has operations distributed across Europe, then the One Stop Shop may assist. It should also be noted that the appointment of a lead supervisory authority does not prevent other supervisory authorities from asserting jurisdiction over matters that concern them, such

as complaints made within their jurisdiction [4]. The details of how these provisions will work in practice remain unclear, but are expected to be the subject of early guidance by regulators.

In order to ensure that the Regulation is enforced uniformly across the EU, the Regulation will require the lead authority to consult with other concerned data protection authorities in cases in which enforcement action by a lead authority affects processing activities in more than one Member State (the “Consistency Mechanism”) [5]. A wide range of issues, such as multijurisdictional enforcement and binding corporate rules, will fall under the Consistency Mechanism.

Extra-Territorial Effect

There is a significant change to the territorial scope of Europe's data protection law. Currently, the EU Data Protection Directive applies to data controllers that are established within the EU, or make use of data processing equipment situated within the EU. In contrast, the Regulation will apply to the activities of a data controller or data processor established in the EU, whether the processing takes place in the EU or elsewhere [6]. It will also apply to processing by a data controller or data processor established outside the EU where the processing relates to the offering of goods or services to data subjects in the EU or monitoring their behaviour in the EU [7]. This will mean that many non-EU businesses, particularly those active online, will find themselves subject to European law. It should also be noted that the Regulation places obligations on data processors, as well as data controllers. For the first time, data processors will be subject to the same range of sanctions as a data controller in the event of a violation of the Regulation.

Breach Notification Requirements

Currently, Europe does not have mandatory breach notification requirements across all industry sectors. There are some industry-specific notification requirements, and a handful of Member States have enacted their own data breach laws, but the position is not uniform. This position will change under the Regulation. In the event of a data breach, an organisation will be required to notify the competent data protection authority without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. There is an exemption from notification where the breach is unlikely to result in risk to individuals' rights and freedoms, for example, where the data are encrypted [8]. Where the breach involves high risks to individuals' rights and freedoms, an organisation must also communicate the breach to the individual without undue delay [9]. Mandatory breach notification, together with the ability for individuals to bring group actions against controllers or processors [10], is likely to transform the data breach landscape, bringing the EU closer to the U.S. breach regime, and making data breach a significant area of risk that organisations will need to prioritise.

Increased Obligations and Accountability

The Regulation introduces a number of requirements designed to make organisations more accountable in their data processing activities. The Regulation specifies detailed compliance requirements for both data controllers and data processors, and requires organisations to implement measures to ensure and to demonstrate, including through the adoption and implementation of appropriate data protection policies, that their processing activities comply with the requirements of the Regulation [11]. Some of these changes are set out below.

- **Current Registration Requirements Abolished** – Requirements to register or notify data processing activities with national data protection authorities will be abolished, but will be replaced by an obligation to maintain internal records [12] of all data processing activities.
- **Maintain Inventory of Data Processing** – Article 28 sets out a detailed list of information that must be included in an organisation's internal data processing inventory. In many cases, these requirements are significantly more detailed than the equivalent national registration requirements under the Data Protection Directive. Organisations will need to give careful thought as to how these records will be created and maintained. They must be available for inspection on request.
- **Lawful Basis for Data Processing** – As is the case under the Data Protection Directive, organisations may only process personal data where they have a lawful basis for doing so. The lawful bases are similar to those permitted under the Directive, but the legitimate interests ground, on which companies in the UK routinely rely, is tightened. The relevant legitimate interests must be set out in the data protection notice provided to individuals [13], and the individual can object to processing based on legitimate interests, including profiling [14].
- **Tighter Requirements for Consent** – Consent will become more difficult to use as a basis for data processing under the Regulation. Organisations that rely on consent will need to review their existing practices carefully and ensure that any consent which they obtain is freely given, specific, informed and unambiguous [15]. Data controllers will have the evidential burden of proving that they have obtained consent [16], which will require most organisations to scrutinise their existing consent mechanisms. “Opt-out” consent, and implied consent mechanisms will need to be updated. Consent will not be considered valid if there is a ‘significant imbalance’ between the parties, for example, in an employer/employee relationship, requiring detailed review of the circumstances in which consent is utilised in an employment context. The Regulation will also introduce a requirement to obtain parental consent to the processing of personal data relating to a child under 16 years of age [17]. Organisations will need to consider carefully how best to achieve this, particularly in an online context where age verification can be difficult.
- **Data Protection by Design and by Default** – The Regulation will require organisations to implement data protection by design and by default [18]. These principles require organisations to take privacy and data protection issues into account from the start of any product design process and during the entire life-cycle of the relevant processing activities, and to properly assess the data protection risks before launching any new products. Data controllers will be required to establish and maintain appropriate technical and organisational measures to implement data protection principles in an effective way and to integrate safeguards for data processing so that, by default, only data necessary for each specific processing purpose is collected. This emphasis on data minimisation should be noted, particularly in organisations embarked on big data projects.
- **Data Protection Impact Assessments** – Data controllers will be required to perform Data Protection Impact Assessments (“DPIA”) [19], where the processing of personal data is likely to result in high risk for the rights and freedoms of individuals. In particular, a DPIA will be required for automated data processing activities, including (i) profiling leading to decisions that produce legal effects for an individual, (ii) where the processing includes large-scale processing of certain types of data, or (iii) systematic monitoring of a publicly accessible area on a large scale.

Contracting with Processors

Unlike the Data Protection Directive (which generally relies on data controllers to contractually flow down compliance obligations to data processors), the Regulation will impose direct compliance obligations on data processors [20]. As with the Data Protection Directive, the Regulation will require that the outsourcing of data processing activities by a data controller to a data processor is governed by a written data processing agreement. Whereas the Data Protection Directive does not specify the content of this data processing agreement, the Regulation mandates in detail the terms that must be included in such a contract. Data processors will be directly liable for the security of personal data during processing activities. As noted earlier, data processors will be subject to enforcement by supervisory authorities in the same way as data controllers for violation of the Regulation.

Data Protection Officers

The designation of a Data Protection Officer ("DPO") [21] will be compulsory under the Regulation where (i) the processing is carried out by a public authority or body, (ii) the core activities of the data controller or data processor require regular and systematic monitoring of individuals on a large scale, or (iii) the core activities of the data controller or data processor include processing sensitive personal data on a large scale, including data relating to criminal convictions and offences. In other situations, a DPO may be appointed by the data controller or data processor on a voluntary basis, and must be appointed where required by EU Member State law.

Enforcement

Enforcement powers under the Data Protection Directive vary considerably in practice. In a significant change, all sectors will be subject to the new enforcement powers, sanctions and penalties that the Regulation imposes. Currently, fines under national law are uneven, and are comparatively low (e.g., the maximum UK fine is £500,000). The Regulation will significantly increase the maximum fine to €20 million, or 4% of annual worldwide turnover, whichever is greater [22]. This higher band of fines is applicable to violation of core provisions of the Regulation, including the need for an applicable legal basis for processing. Additional powers include the power to audit data processing activities, which will be new in some jurisdictions, such as the UK. The Regulation will harmonise the approach to enforcement across the EU although, of necessity, there will continue to be variations in practice under local law. Further, the Regulation will make it easier for individuals to enforce their rights [23]. Individuals will have the right to lodge a complaint with a supervisory authority [24], obtain a judicial remedy against a supervisory authority [25], or obtain a judicial remedy against a controller or processor [26]. As noted earlier, where there has been a breach of the rights of data subjects, any association or body acting in the public interest will be able to bring a claim on behalf of affected data subjects under the Regulation, somewhat similar to U.S. class actions.

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 that it is no longer necessary to process, where consent has been withdrawn or where the individual objects, but also to inform recipients of the data that the individual requires those data to be deleted. Individuals will also have a new express right of data portability. This will require controllers to provide personal data in a structured, commonly-used and machine-readable format to individuals. Individuals will also be able to request, where technically feasible, that the data controller send his or her personal data to another data controller, making it easier for consumers to switch between service providers. In addition, individuals will have greater informational rights (including the right 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 automated processing, such as profiling, that produces legal effects for individuals or otherwise significantly affects them.

What Should Organisations Do Now to Prepare?

Start Now!

Many organisations are unaware of the significance of Europe's new data protection laws, or of the extent to which their businesses may be affected. While there have been numerous media headlines about the levels of fines that supervisory authorities will be able to impose, and about the more controversial aspects of the right to be forgotten, many of the changes that form part of the Regulation are much more mundane, and do not merit media headlines. However, organisations need to get into the detail of these seemingly straightforward tweaks and amendments and consider the impact of these changes on their individual organisations. It is quite likely that some of these seemingly small amendments to the legislative text will have a big impact on internal processes, and take time to implement.

Many organisations have been working for some time to analyse what the Regulation will mean for them, and have been planning change projects to implement the required changes to their processes. It is by no means too late to start, but organisations should be aware that the longer they wait, the more they will have to compete for external legal and consultancy support. All organisations will have work to do in order to prepare for the Regulation, and there is already a sense that knowledgeable external legal advisers and consultants are busy.

Where to Start?

It is tempting to start by analysing the Regulation, but the better starting point is to verify existing personal data assets and how they are used within an organisation, for what purpose, with whom they are shared, and what the current data protection programme consists of. Without taking stock of these basic facts, a great deal of time can easily be wasted. The composition of the existing data assets will help to identify key risks and to prioritise remedial tasks.

The data diligence phase can be conducted by devising a basic questionnaire that addresses the following broad topics: data collection (including notice); data processing (legal basis); purpose limitation; data minimisation; data quality; data retention; individual rights; data security; service providers; international data transfers; and works councils. Once this core information is collated from across the business, it must be assessed in order to evaluate the current state of compliance. This should provide a good foundation for the work that will need to be undertaken to ensure compliance

with the Regulation, particularly in those areas where the new requirements represent only a small change to the position under the Directive.

Analysing the Regulation

The second phase of activity is to identify which of the changes in the Regulation will impact the organisation, and what changes will need to be made to the company's existing data protection compliance programme. Based on an assessment of this sort, the organisation will be able to create a list of remedial activities, and begin to prioritise them for action.

Analysing the Regulation may seem daunting, but a number of organisations have approached this task by breaking down the requirements into manageable topics, which are then discussed in detail with relevant business colleagues. It is crucial that those responsible for the operation of business processes are engaged in these discussions. Key topics to consider include the following: definitions; territorial scope; key principles for processing; legal basis for processing; sensitive personal data; privacy notices; individual rights (access, rectification, erasure, restriction of processing, portability, objection, automated decision-making (including profiling)); controller/processor responsibilities; data protection by design and by default; data protection impact assessments; security; breach notification; and cross-border data transfers. Under each of these topic headings, organisations need to understand what the new requirements are, and how they differ from the position under the Directive.

Gap Analysis

The next step is to assess existing compliance against the requirements of the Regulation, and devise specific steps to address any gaps. This gap analysis is a critical step, and a thorough approach is required so that the organisation can then prioritise key remedial tasks. It is only by descending into the detail of the legislation that an organisation will have a true sense of the magnitude of the remedial actions that lie ahead.

Creating Implementation Plan

Once the remedial activities have been identified, the organisation will need to prioritise tasks for implementation. Those that require a lengthy implementation period will need to be planned accordingly. Otherwise, some organisations may prefer to action a number of easy, "quick wins" at the outset. Remaining tasks will need to be scheduled for attention having regard to the importance of the issue, the amount of time likely to be required to address the issue, and available resources.

The data protection team will need to engage the support of others in the organisation to plan and implement required changes. The volume of work, the technical complexity of some of the tasks, and the need for the organisation to play an active role in ensuring that any changes work from an operational perspective, all point to the need to engage additional resources, both internal and external. The data protection team will play a key role in managing the project, and evaluating the implementation, but some organisations are also requiring operational teams to take responsibility and report progress with implementation to regular meetings of the compliance committee. Such a reporting structure may help to ensure that preparation for the Regulation has sufficient internal visibility.

Key Tools for Managing Privacy Risk

In addition to planning for implementation of the Regulation, organisations must consider how they will maintain their data protection compliance programme on an ongoing basis. Key tools to assist with this include the appointment of a DPO, an ongoing focus on the structure and content of the data protection compliance programme, and considering how to adopt a risk-based approach to data protection that, beyond legal compliance, reflects an individual organisation's risk appetite and culture.

Appointing a Data Protection Officer

Many organisations are seeking to appoint DPOs, even where they are not mandated by the Regulation. DPOs can 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.

The detailed responsibilities of a DPO will vary from one organisation to another, but the key focus of the role is to oversee data privacy compliance and to 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 organisations assess new business opportunities that utilise data assets.

Where mandated, the Regulation specifies the tasks that a DPO is required to undertake. First and foremost, a DPO is expected to advise the controller or processor about their compliance obligations under the Regulation, and to monitor compliance with the Regulation, other applicable data protection requirements, and internal data protection policies. The DPO will provide advice on data protection impact assessments, cooperate with the supervisory authority, and act as a contact point for the regulator. Finally, the Regulation specifically requires the DPO to have regard to the risks associated with particular data processing activities; such as the nature, scope, context and purposes of the processing.

Data Protection Compliance Programme

As organisations prepare for implementation of the Regulation, they should also look to their broader privacy compliance framework to ensure that work to implement the Regulation is embedded in that framework.

Typically, a privacy compliance programme will 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 components of the programme include: policies and processes; people; and technology to help manage data protection compliance.

- *Policies and processes* constitute the rulebook which describes the organisation'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 organisation, and the DPO, to identify and calibrate privacy risk.
- *People* are key to implementing the organisation's data privacy rulebook. 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 organisation's approach is, and why the organisation thinks data protection is important. The DPO can play a key role in raising awareness and rolling out training.
- *Technology* refers to systems and automated controls. The DPO needs to work with the organisation's IT and Information Security functions to ensure that systems operate in a privacy-compliant way, and that data security is ensured.

Risk-Based Approach

It should also be noted that the Regulation proposes a risk-based approach to compliance, under which organisations will bear responsibility for assessing the degree of risk that their processing activities pose to individuals. Adopting a risk-based approach to compliance does not alter rights or obligations, but is a valuable tool that organisations can utilise to demonstrate accountability, prioritise actions, raise and inform awareness about risk, and identify appropriate mitigation measures. The goal of a risk-based approach to compliance is to reduce the risk as far as is practical but to be explicit about the remaining risk, and how it will be managed. By adopting a risk-based approach to the entire life-cycle management of personal data, from collection to processing to deletion, an organisation can achieve a scalable and proportionate approach to compliance. 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.

Conclusion

As European data protection law is reformed, existing legal requirements will be tightened, and sanctions strengthened. Fines of up to €20 million, or 4% of annual worldwide turnover, will be available under the new regime. Now, more than ever, organisations need to manage data privacy risk proactively. There is no time to

lose. Organisations must begin to consider what the Regulation will mean for them, and start to assess their compliance posture, so that remedial tasks can be identified and targeted in good time. In a world in which personal data processing underpins so much business, social, charitable and public sector activity, and where individuals are increasingly aware of their data protection rights, these tasks cannot be left to chance. An organisation's reputation is increasingly tied to how well they respect and take care of the personal data that they process. The time has come to begin preparations for implementing the Regulation.

Endnotes

1. A copy of the consolidated text is available at: http://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf.
2. The discussion in this chapter focuses only on the Regulation.
3. Article 51a(1) of the Regulation.
4. Article 51a(2a) of the Regulation.
5. Articles 57–62 of the Regulation.
6. Article 3(1) of the Regulation.
7. Article 3(2) of the Regulation.
8. Article 31 of the Regulation.
9. Article 32 of the Regulation.
10. Article 76 of the Regulation.
11. Articles 5 and 22 of the Regulation.
12. Article 28 of the Regulation.
13. Article 14(1)(c) of the Regulation.
14. Article 19(1) of the Regulation.
15. Article 4 of the Regulation.
16. Article 7 of the Regulation.
17. Article 8 of the Regulation.
18. Article 23 of the Regulation.
19. Article 33 of the Regulation.
20. Articles 28–31, 33–35 and 40 of the Regulation.
21. Articles 35–37 of the Regulation.
22. Article 79 of the Regulation.
23. Articles 53, 74, 75 and 77 of the Regulation.
24. Article 73 of the Regulation.
25. Article 74 of the Regulation.
26. Article 75 of the Regulation.

**Bridget Treacy**

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

Tel: +44 207 220 5600
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 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' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by *Computerworld* for four consecutive years as the top law firm globally for privacy and data security. *Chambers & Partners* ranks Hunton & Williams as 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.

This article presents the views of the author and do not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.

This article appeared in the 2016 edition of The International Comparative Legal Guide to: Data Protection published by Global Legal Group Ltd, London. www.iclg.co.uk

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks



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