Osborne Clarke is one of Europe's most respected law firms and a UK leader in advising marketers on the legal issues affecting them. The firm's MarketingLaw .co.uk website has provided marketers with authoritative legal insights for over 10 years. Please send any queries regarding this column to Stephen Groom (stephen.groom @osborneclarke.com)

Legal and Regulatory Update

EU data privacy laws face big shake-up

James Mullock

Journal of Direct, Data and Digital Marketing Practice (2012) **13,** 369–371. doi:10.1057/dddmp.2012.6

Topic: Privacy
Who: The European Commission
When: January 2011
Where: European Union
Law stated as at: 31 January 2012

What happened

European Commission (EC) re-write of data protection laws proposes fines of 2 per cent or world-wide turnover.

Most people would agree that Europe's data protection regulatory regime desperately needs an overhaul. The current laws originate from a Directive written in 1995 in a pre-cloud computing era, before offshoring, globalization and digital business practices became key business concerns.

Since 1995, new data protection laws have been layered upon one another as law makers have desperately sought to keep up with technology developments. The result is widely seen as over-bureaucratic, with too much focus on registrations and filings. The EC has made no secret of its desire to overhaul the European Union's (EU) data protection regulatory regime. Recently, its botched attempt to introduce new cookie/tracking technology laws in a harmonized way has led to an additional desire for a single set of EC-drafted laws to apply across Europe.

In a new draft Regulation published on 25 January 2012, the EC set out the new laws that it would like to be introduced. Once these have passed through the European parliamentary system, because they are in the form of a 'Regulation' they will have direct effect in every EU Member State with minimal further scope for debate, or rationalization. While a more harmonized data protection regulatory landscape sounds appealing, the uncompromising approach taken by the EC's draft Regulation is a cause for concern for business.

Key points proposed by the EC's draft Regulation include the following:

(a) *Fines* — National data protection regulators will be given the ability to impose significantly higher fines of up to 2 per cent of global turnover where basic knowledge/consent obligations or requirements to adopt good policies and procedures are not followed.

(b) *Data protection officers (DPO)* — Private sector companies with more than 250 employees, or whose core activities involve regular monitoring of individuals, as well as public authorities will all be required to formally appoint a DPO. The DPO must be empowered by their organization to act as an independent assessor of its compliance with data protection laws and report to the board of directors in doing so. The Regulation specifically requires the DPO to coordinate data protection by design and privacy impact assessment (PIA) initiatives (see below for more details on both) and to be responsible for data security initiatives generally. Responsibility for training staff is also mentioned as important. In short, the DPO must ensure that his/her organization has adopted good data governance policies and procedures.

(c) *Audits, data protection by design and PIAs* — Organizations will be required to demonstrate that they have undertaken regular data protection audits and PIAs using recognized industry standards (such as the Information Commissioner's Office's PIA criteria). Key to achieving compliance will be an ability to demonstrate that new processing systems and activities have only been introduced after privacy compliance and risk mitigation steps have been implemented. A key role of an organization's DPO will likely be coordinating such privacy by design initiatives. Regulators will be empowered to designate processing activities in respect of which organizations should always proactively run a PIA before processing commences. The Regulation sets out a starting point list that includes any activities using data about an individual's 'economic situation, location, health, personal preferences or reliability of behaviour'.

(d) *Security breach notification* — Organizations will have to notify data protection authorities within 24 h of establishing that they have suffered a data breach or explain why it is not possible to provide full details of the breach. Slick internal procedures will therefore be required to verify suspected breaches and establish what has been lost or subject to unauthorized accessed.

(e) *Expanded consent requirements* — The EC's proposals include a radical overhaul of the level of consent that is required before organizations process data. At the heart of this change is the requirement that consent to use personally identifiable information always be obtained in advance and on an opt-in basis before it is used. Thankfully the EC has pulled back from requiring parental consent to be obtained from those under 18 years of age, as required by an earlier draft of the Regulation leaked in November. The bar is proposed at 13 years of age in the draft Regulation published in January.

(f) *Data portability* — Individuals will be given the right to demand that an organization transfer any or all information held about them to a third-party organization in a format that the individual determines. This increases the control that individuals have over data that identify them, and makes it easier for them to transfer

business or employment relationships. It remains to be seen who will be required to cover the associated costs of such an exercise, but it seems very likely that the transferring organization will be expected to do so.

(g) *Jurisdictional reach* — The new laws will apply to anyone processing data in the EU, as well as those outside Europe who offer goods or services to EU citizens. For a multinational organization, the location of its European HQ will determine which EU Member States' laws bind it, and which regulatory authority will have jurisdiction over it. That said, individuals will be given wider-ranging powers to bring action personally against an organization (either in the country where a non-compliant organization is located or in the individual's local courts). Trade associations will also be empowered to bring class actions on behalf of their members. For the first time, data processors will share equal responsibility and liability for compliance with the new laws, raising the stakes for IT service suppliers.

(h) *Data transfers* — Europe's painful data transfer laws will be relaxed in that more options will be made available to enable organizations to share data with non-European third parties. Specifically, the policy implementation known as Binding Corporate Rules will be formalized as a mechanism enabling data transfer compliance, which is good news for multisite, multinational businesses.

(i) *The right to be forgotten* — Individuals (children, defined as under 18 years of age, are mentioned in particular) will have the ability to demand that information published about them online is deleted and is not republished. Organizations that receive such a demand must take all reasonable efforts to inform other website operators of the existence of the complaint that they have received. The right, which is particularly relevant to social media businesses, is subject to some exemptions. These include one benefiting journalists publishing stories in the public interest, raising the question as to whether a blogger or someone who posts an opinion on a website is a journalist. But questions remain about how practical the regulation is and who would bear the costs of complying with it.

Why this matters

The EC has set a 2-year timetable for implementation of its proposals through the European parliamentary system. For UK businesses attention now turns to the Ministry of Justice to see what stance it will take in negotiating (on the UK's behalf) the final form of the Regulation.

For more details about the EC's proposals and for a copy of our guide to complying with data protection laws.

James Mullock, Partner, Osborne Clarke, Bristol
james.mullock@osborneclarke.com