Ardi Kolah

is a respected PR, marketing, sponsorship and internal communications practitioner.

He is a Fellow of the Chartered Institute of Marketing and the Chartered Institute of Public Relations, member of the Public Relations Consultants Association, and chairman of the Law and Marketing Committee for the Worshipful Company of Marketors.

Bryan Foss

worked at IBM for more than 26 years in technical and international executive roles.

More recently, he has built a portfolio of independent director roles, currently including international technology and financial services organizations. He is an active Fellow of the BCS, an IoD chartered director and a Visiting Professor at Bristol Business School.

Martin Hickley

is a leading data governance, protection and privacy specialist with 25 years' experience mediating with regulators in the world of data and information, working in blue-chip companies where data is the *raison d'être*. Experienced in data management, data governance and privacy/risk/compliance/security, he takes a global and enterprise view of how data should meet all known current and future business objectives within the evolving regulatory framework.

Keywords: data protection, data governance, privacy

Important stuff for UK marketers

Ardi Kolah,
GO DPO EU Compliance Limited,
71-75 Shelton Street, Covent Garden,
WC2H 9JQ, London
Tel: +44 077100 77941;
E-mail: ardi@godpo.eu

Opinion Piece

What should UK and US marketers do to prepare for the biggest threat to business continuity for a decade?

Ardi Kolah, Bryan Foss and Martin Hickley

Received (in revised form): 7th October 2015

Abstract

Marketers in the United Kingdom and the United States need to be aware of the provisions being considered as part of the European General Data Protection Regulation. As soon as it is agreed and becomes law, many current practices will cease to be legal. This article outlines what marketers need to be doing in 2015 in order to be ready for this major change in data protection law.

Journal of Direct, Data and Digital Marketing Practice (2015) **17**, 86–92.
doi:10.1057/dddmp.2015.50

All change in data protection

By the end of 2015, the way in which all marketing that has personal data at its centre and is conducted within the European Union will have changed forever as a result of the EU GDPR. This new EU Regulation will clear away existing data protection, privacy laws and regulations across every Member State, with the result that this branch-and-root reform will strike at the existence of many existing direct marketing activities that simply don't comply with the new principles enshrined under the GDPR.

At a stroke this one EU Regulation will update the former Data Protection Act principles and the previous EU Data Protection Directive. In fact, the new EU Regulation is three times longer than the Data Protection Act 1998. Marketers on both sides of the Atlantic will have a 2-year transition period in order to mitigate any actions that will be taken for personal data breaches once the transition period expires. With fines being set between 2 and 5 per cent of annual global turnover in a consecutive 12-month period, commercial organizations simply can't afford to ignore this new EU Regulation as it presents the biggest threat to business continuity for a decade.

This can be summarized as follows:

- Putting individuals back in control of their own data
- Opt-in consent for marketing
- Portability of data
- Mandatory breach notification

- More effective supervision and enforcement
- ‘One-stop shop’ for complaints.

Putting individuals back in control

This includes moves for explicit consent required for the use of data, the so-called ‘right to be forgotten’ and powers to take legal action against organizations that don’t respect these rights by complaining to the Supervisory Authority, rather than going through the court system.

Opt-in consent for marketing

Under the new rules, consumers will have to opt in to direct marketing from a company and the resulting pool of people available to marketers will be reduced when compared with opt-out marketing consent used in the past.

Portability of data

Data portability is essentially about allowing users to extract, in a structured electronic format, personal data from service providers and to move that data to another provider. This idea stems from existing practices in the mobile telecoms and banking sectors (current accounts) and it’s about giving more say to individuals to decide what happens to their data in practice and being able to effectively make a choice of supplier in the market. According to the European Commission, this measure lowers the barriers to entry, in particular to those markets that are currently dominated by very few big players.

Mandatory breach notification

In this area, the European Commission has studied in detail what some states and federal bodies in the United States have adopted in terms of personal data breach notifications to the consumer and is convinced of the case for a federal approach across the EU. This approach is consistent with what’s known as ‘protection of privacy by design’, which means it’s about marketers investing in good data protection practice and methods as early and as upstream as possible in the provision of goods and services.

More effective supervision and enforcement

The new emphasis on supervision and enforcement placed by the European Commission reflects the transition from an *ex-ante* to an *ex-post* data protection and privacy system. Data protection and data breaches have become much more serious and relevant and, currently within the EU, there isn’t a credible set of enforcement rules and sufficiently dissuasive sanctions — for example, there will be over 20 types of administrative fines, whereas now there are just two under the current regime. In fact, enforcement is currently very fragmented, where some countries have power to impose financial penalties and some countries don’t appear to have that power.

Proportionality of fines

The change in supervision and enforcement draws from the experience of competition law. The level of fines — up to 5 per cent of global turnover or €100m, whichever is the greater — is a maximum and will be applicable to the most serious violations of the GDPR where the principles of proportionality will apply, and this includes the impact of a data breach on users. From a marketing and PR perspective, any public sanction carries the risk of damage to a company or organization’s reputation, so marketers must ensure that all data that is being used in marketing activities complies with the GDPR.

‘One-stop shop’ for complaints

The idea of a ‘one-stop shop’ is to make it easier for citizens within the EU to complain about infringement of their data protection and privacy

rights under the GDPR. However, not everyone in the EU likes this and the Council of Ministers in particular isn't keen, but it could yet be won over to back this change as its a centrepiece of the GDPR as drafted by the European Parliament.

Data Protection Authorities

The way it works is as follows:

- When the decision involves measures to be taken *vis-à-vis* the data controller, the imposition of a fine, injunction or a move to put an end to certain processes, then that decision is jointly agreed and will be formally adopted by the Data Protection Authority (DPA) of the main establishment
- When the jointly agreed decision has a negative impact on the individual by rejecting their complaint, it will be adopted by the local DPA and, in that way, it ensures that the decision can be challenged before a domestic court in the country of the complainant.

Fundamental rights

Where the local DPA isn't able to reach agreement with the DPA for the main establishment, the matter will be referred to the European Data Protection Board and that decision will be binding on all parties. According to the European Commission, this is a legally more robust position under the perspective of the Fundamental Rights Charter.

Practical stuff to consider doing now

Don't sit on your hands and adopt a 'wait-and-see' approach. And don't think 2 years as a transition period gets you off the hook from doing anything now — doing nothing will be viewed as an aggravating factor by the Supervisory Authority (the Information Commissioner's Office in the United Kingdom) in light of any subsequent personal data breach. Imagine you're a company and the data controller. You know that, once the GDPR is approved, you'll have a 2-year grace period in order to ensure that all data protection and security procedures comply with the principles of the EU Regulation.

Contracting third parties

Two years is a shorter period of time compared with the average length of most business and marketing contracts, so the implications of the GDPR take effect not in some distant point in time, but from today, as policies, procedures and contracts are updated. For example, all contract renewals and new contracts that entail personal data transfer or processing will need to have a clause in them that effectively says that, once the new EU Regulation is passed, the third party has to supply to you within a set time frame its plans to become compliant with the GDPR. As many companies now outsource operations that use customer data, this will prove to be a common issue to address.

Breach notification timescales

Furthermore, you might need to re-negotiate the third-party contract based upon those plans, due to cost and liability issues. For example, we know there will be a statutory requirement to declare a personal data breach within a very short time-frame, so the third party will need a formal process to tell you that they believe there's a breach and this is what you have to consider and report.

Responsibility of the data controller

Timescales are short because it's a two-company process. But who's responsible if the deadline isn't met? The answer is simple — it's you as the data controller. Which is one reason why the CEO of T-Mobile, John

Single breach, multiple fines

Legere, publicly expressed his anger at the announcement that Experian, the world's largest credit rating agency, had suffered a sensitive personal data breach affecting 15 million T-Mobile customers after its servers were hacked.

What penalties do you accept and what do you pass onto the third party in such circumstances? This can only be clear if it's provided for in the contracts that you are entering today that have more than a 2-year shelf-life. Imagine that a data processor has a single data breach, but the data is on multiple records. The fine will not be for one breach, but multiple breaches under the GDPR.

Important stuff for US marketers

America's biggest corporations generate vast profits from their marketing activities with EU citizens. Under the GDPR, US-based companies that have never set foot within the EU will face significant fines of between 2 and 5 per cent of global turnover if they refuse to play by the new rules. This may sound like a nightmare scenario, but data protection and privacy laws across the largest single trading block in the world are just about to get harmonized. There are several drivers for these changes and the big one is definitely privacy. Interestingly, the word 'privacy' doesn't appear in the US Constitution. However, like the right to carry arms that so many Americans feel defines their version of democracy, millions of Europeans consider their right to privacy of their personal information to be just as sacred and to be a fundamental human right.

Privacy enshrined in law

European experiences in the last Century, where personal information was extensively used for totalitarian, discriminatory and genocidal purposes, may be at least partially responsible for an array of national laws enshrining a right to privacy, as well as supra-national protections, beginning with Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and Protocols in 1950 and, more recently, the EU Data Protection Directive of 1995.

Varied laws across the EU

The EU Directive, which is still in force until the GDPR has been agreed (possibly as early as the end of November 2015), established a broad set of principles with respect to the protection of privacy and personal data. However, each EU Member State was given wide discretion to implement these principles at a national level, with the result that US companies faced a patchwork of data protection and privacy laws. This made it very difficult to work out how to run marketing campaigns across the EU without the fear of falling foul of data protection and privacy laws that varied between different jurisdictions. The legacy is that, today, EU privacy and data protection laws are far from uniform and their impact on commercial activities varies greatly, which is one reason why these will be swept away by the forthcoming GDPR.

Cross-border transfer of data

Given the landmark ruling of the European Court of Justice (ECJ) this month (October 2015) that invalidated the long-standing Safe Harbour agreement between America and the EU, companies like Facebook, Google, Amazon, DropBox and Salesforce.com must now, as a matter of urgency, review how data is transferred in accordance with the ECJ ruling. The unpredictability of the application of data protection and privacy laws across all 28 Member States has just become much more unpredictable, leading some to push for the GDPR to be signed off as early as the end of

Lawful data transfers essential

October 2015 in order to restore harmonisation, consistency and clarity for all companies affected by the ECJ decision.

Antony Walker, deputy CEO at techUK, described the ruling as ‘hugely significant’ and said it will cause real confusion and uncertainty for all sorts of businesses that need to transfer data between the EU and the United States. According to Walker, ‘Businesses will be looking to the European Commission and national data protection authorities to steady the ship and provide clarity on what they need to do to ensure their transatlantic data transfers are lawful. This is a big issue for many small businesses, in particular, which will be faced with the time-consuming and costly task of working through the full legal implications. The ability to transfer data lawfully across borders is fundamental for a growing and dynamic digital economy. Businesses need stability and certainty in the legal framework that enables this to happen’.

Encryption keys

All organizations must ensure they can keep company and customer data private, even when backed up into a public cloud. Pseudonymisation and encryption of data before it leaves the endpoint device, so that it cannot be decrypted in the cloud and hence remains private, will be necessary in order to comply with the ECJ’s ruling. Some of the best security technologies available will be encryption keys that are kept by customers so that only they can decrypt the data and to which no one else has access without a prior direct request.

Safe Harbour alternatives — model contracts

An alternative to Safe Harbour has been Model Contracts. These are forms negotiated between the US Commerce Department and the European Commission that can be used when personal information is transferred from the EU to the United States. These documents typically can’t be modified to suit the business transaction and this inflexibility can sometimes be a barrier to their use.

Binding corporate rules

A very few organizations have implemented ‘binding corporate rules’ (BCRs) that allow multi-national corporations, international organisations and groups of companies to make intra-organisational transfers of personal data across borders in compliance with EU Data Protection Law. The rules must conform to strict protocols, and be approved by multiple data protection agencies in Europe. The time, cost and expense of enacting BCRs has slowed adoption by even very large companies, which is why the GDPR will become *de facto* the way in which data transfers will now be regulated, with the objective of harmonisation across the European Union, sweeping away the wide variety of rules and regulations among EU Member States and replacing them with a uniform set of principles.

A game-changer for US marketers

At first glance, the concept of uniformity is extremely attractive. This new EU Regulation has been regularly promoted as a means to simplify conducting business in Europe. However, the devil is in the detail and especially with respect to how the GDPR will be implemented. A central driver behind the introduction of the new EU Regulation is to enhance affirmatively protections for individuals and their data — which will entail an inevitable and, in some cases, potentially dramatic increase in the regulation of companies, not to mention substantial increases in the potential financial penalties.

Joint liability

US companies will be the controllers of personal data that belongs to the data subject and will also be responsible for directing the use of that data by processors. There may be situations where US companies will be working jointly with processors for different purposes. Legal liability for ensuring protection of the data typically rests with the controller (although controllers may have claims against processors for data misuse, breach and so on). The GDPR proposes a significant change in this framework, establishing that controllers and processors may be jointly and severally liable for personal data breaches or other unauthorised use and/or disclosure of personal data, including direct claims by the affected data subjects.

Google versus González

From a commercial perspective, this new approach has the potential to complicate immensely routine transactions. A vivid example of the impact on commercial operations can be seen in last year's Google Spain versus AEPD and Mario Costeja González (http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065) case in the EU Court of Justice that effectively established the concept of 'the right to be forgotten', now part of the forthcoming GDPR. A Spanish citizen filed suit when a Google search of his name disclosed publicly available information regarding past financial difficulties. González argued that a 15-year-old reference should not appear at the top of search rankings for his name. The ECJ agreed and forced Google to implement a process for individuals to request that links to information be deleted from search results, a daunting task since the opinion provided little guidance on the limits of the 'right to be forgotten'. However, as of now, the results of the same Google search conducted in the United States and in the EU may be different.

Data protection officers

US companies that are doing business with EU citizens right now need to get on and carry out a data protection impact assessment across their entire operations, not simply on a project-by-project basis. They also need to appoint a data protection officer (DPO) who will effectively be the eyes and ears of the company and 'in-house regulator' on how it complies with the GDPR. Under the GDPR, the DPO enjoys a very different status to senior managers, given that his/her primary responsibility is to protect data privacy rather than advancing the commercial interests of the company at any cost.

Reporting data breaches

The forthcoming EU Regulation includes draft language with respect to rapid reporting of personal data breaches within 24 hours, although a proposed modification would increase the time frame to 72 hours. This will pose a significant burden as many organisations are simply not geared up to respond to unplanned events in such a short time-frame. In addition, there is no de minimis as all data breaches will need to be reported to the Supervisory Authority, whether or not they cause harm or distress to the data subject.

Impact on internet marketing

Internet marketing — the very model that's inextricably embedded in countless commercial practices and increasingly sustains commercial activity on the internet — is at risk under the GDPR. Specifically, profiling — the practice of developing a snapshot of an individual's preferences, browsing history, purchases and so on — is at risk as an individual would have the right to object and stop profiling, unless it is necessary to perform

under an agreement, authorised by law or has been explicitly consented to by the individual.

Behavioural targeting

Behavioural advertising, targeted marketing or remarketing, email solicitations and other direct marketing practices will be less effective if they can't be targeted using individual profiles, rendering them less valuable. The collection of information on individuals as a basis for displaying personalised ads — one of the largest tools in the current toolbox of e-commerce — could suddenly disappear.

Not if, but when

The question is not whether, but when (and how) the EU Regulation is going to pass. Currently, the European Commission, the European Parliament and the Council are attempting to reach agreement on the final wording of the GDPR behind closed doors. But all indications are that agreement could be reached as early as the end of November 2015 and then US companies will need to change how they market under the 2-year transition period. So, if you're reading this and are a marketer based in the United Kingdom or the United States, time is very much of the essence.