Prioritising Privacy

This article was originally published in the October 2014 issue of *Managing Partner*.

by Rafi Azim-Khan

Rafi Azim-Khan
Intellectual Property, Data Privacy, Marketing
+1.44.20.7847.9519
rafi@pillsburylaw.com

Rafi Azim-Khan is head of Pillsbury's Data Privacy practice in Europe and leads the firmwide Marketing Law Team. He is a partner in the Intellectual Property and Information Technology practices.

Law firms and clients that are caught unaware of changes to international data protection legislation risk heavy fines.

New laws, fines and increased enforcement activity mean that staying on top of data protection issues is now more important for businesses than ever before.

Perhaps it is unsurprising that many businesses have traditionally taken a somewhat half-hearted approach to data protection/data privacy (DP) compliance.

In the UK, a mix of historically small fines and seeming lack of enforcement by the Information Commissioner's Office (ICO) had, until recently, created an environment in which DP issues were often regarded as lower priority.

However, numerous factors have been coming together in recent months, including new laws, fines, enforcers and EU-wide/ global proposals, which mean that such an attitude is now very much outdated.

Important DP law changes affect not just UK or European companies and firms, but also any that are deemed to be 'processing' data in Europe. Law firms and their clients, wherever they are based, must now react to the changing conditions or else find themselves potentially unprotected and exposed to greater risk.

Higher UK Fines

Fines for serious breaches have increased significantly in the UK, with each offence now potentially punishable by a fine of up to £500,000. These new fine levels are not theoretical. Recent six-figure fines levied by the ICO include ones of £440,000, £250,000 and £325,000. For those who remember fine levels at around the £5,000 mark, this represents a sea change.

Fines in other EU states, such as Spain, France, the Netherlands and Germany, can be equally significant. For example, the producers of the Spanish version of Big Brother were fined more than €1m for data protection breaches.

New EU Privacy Laws

A new E-Privacy Directive was implemented in Europe relatively recently, changing legislation on the use of cookies, customer profiling and data tracking, among other things.

In summary, users must provide consent more clearly before their data can be processed, changing the way that websites operate. There have been important EU Working Party clarifications on requirements to secure explicit, rather than implicit, consent. There has also been much confusion and debate over what is or is not sufficient and, even now, many business websites (including those of some law firms) are arguably not compliant.

Such new legislation increase the chance that otherwise compliant companies and firms may be caught out as the goalposts move. The regulators have given businesses a grace period thus far, but we will now start to see more enforcement.

In addition, an even more significant new regulation, to replace the current Data Protection Directive, is on the horizon. The current draft European Data Protection Regulation has the strong backing of the European Parliament and is expected to be implemented by the end of 2015.

One of the most significant announcements under the new European Data Protection Regulation is the proposed introduction of even larger fines: up to five per cent of global turnover/ revenue for a serious breach of DP legislation. Companies and firms should, therefore, prioritise identifying what may need attention.

In particular, organisations should urgently review their data processing activities, particularly where:

1. personal data is processed in Europe (i.e., collected and stored);
2. personal data is transferred outside of Europe;
3. cookies are used on websites that target European users; and
4. marketing communications are sent to Europe.

Websites and Social Media

One of the main reasons that there is increased collection and use of data—especially via websites and social media—is the desire to process it for more targeted marketing purposes.

This has driven another recent enforcement change to note. The rules surrounding social media activity and websites have become more complex, not least because regulatory codes that did not previously apply have now been extended.

For example, in the UK, this has resulted in the Advertising Standards Authority (ASA) having its remit extended so that it now also includes policing websites and social media activity. The new information commissioner was in fact previously at the ASA, and something flagged by the watchdog can equally be brought to the attention of the ICO.

Companies and firms should, therefore, review their websites and examine how they capture/use all data, including data obtained via social media platforms such as Twitter and Facebook.

Privacy by Design

The new European DP regulation also includes the concept of 'privacy by design'. This has been a key mantra coming out of the European Commission. Essentially, companies/ firms must now demonstrate that they are taking DP more seriously.

When investigating a violation, enforcers are unlikely to have much sympathy for organisations that have taken a lackadaisical approach to compliance. Conversely, demonstrating that efforts have been made to update old DP policies and to retrain employees should help to reduce the risk of fines.

International Data Transfers

An area currently under scrutiny is that of international data transfers. It can often be a problem area, with data being sent unlawfully to countries not deemed adequate (for instance, the US). Companies and firms with global operations will be fully aware of the challenges faced from a data compliance perspective associated with the transfer of client and employee data across borders.

So, what exactly is the best solution for a business needing to handle and transfer personal data across jurisdictions? This has become an increasingly important and common question as firms become more global and grow, reorganise or merge.

There has been a lot of discussion recently about the best way to adequately safeguard personal data which is transferred out of the European Economic Area (EEA), thereby ensuring that transfers are compliant with European data protection laws relating to extra-EEA transfers. Similar debates have taken place outside of Europe, often resulting in conflicting views on what one should be doing across the board and a patchwork, global approach to compliance.

Many commentators, including some of the key European regulators, have said that there remains a lot of confusion and misinformation surrounding the pros and cons of the various routes used to ensure cross-jurisdictional transfers are compliant.

As a result, earlier this year, the EU Working Party published a comprehensive opinion for the first time, working along with its counterparts from the Asia-Pacific region, with the aim of assisting international businesses that are struggling to come to terms with increasingly complex global data privacy laws and enforcement risks.

What all this means is that, while multinationals sending data outside the EEA have a range of options to ensure their transfers are compliant, the solutions and the pros/cons of each are changing.

Using Safe Harbor

One route which has in the past been popular (although sometimes a little misunderstood and misused in practice) is 'Safe Harbor'—a scheme to permit data transfers from Europe to the US. In recent times, this has been the subject of criticism, challenge and some doubt.

In particular, partly prompted by the Snowden saga, reports as to government surveillance and growing concern over what is happening to data that is transferred overseas (particularly to the US), the EC published last year a series of recommendations that it said the US Department of Commerce (the administrator of the nationís Safe Harbor Program) should respond to, or else the programme might be suspended. The EU essentially stated that it was not convinced that US companies and the US administration were respecting data or the Safe Harbor Program.

These recommendations, in summary, relate to greater transparency on the part of the adhering companies and stricter enforcement.

In response, the US administration has stood its ground on a number of aspects to defend its Safe Harbor Program and has cautioned that not all of the reforms proposed by Europe will be workable.

Given such posturing, a cloud has arguably been cast over the future of Safe Harbour and, while it remains unclear whether suitable agreement across the Atlantic will be reached, there would appear to be considerable merit in considering an alternative solution.

Developments in BCRs

Disadvantages associated with the use of model contract clauses (one alternative route to permit data transfers), in addition to concerns over Safe Harbor, mean that binding corporate rules (BCRs) are now becoming increasingly popular among multinationals.

While the previous BCR regime was not that popular, given the perceived slow speed and heavy workload, that view is now outdated for various reasons, such as the introduction of the mutual recognition process. This has significantly streamlined the process and made it an altogether more attractive option.

In 2014, the attractiveness of BCRs increased further as a workable solution to ensure global compliance. The EU Working Party launched an opinion (02/2014) on "a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents".

In short, for the first time, we now have a practical checklist and comparative tool (the Referential) to help businesses to comply with confusing global transfer requirements. Endorsed by both the EU working party and the Asia-Pacific Economic Cooperation's data privacy sub-group (the working party's counterpart in the Asia Pacific region), it sets out the respective requirements when seeking BCR and/or cross-border privacy rules (CBPR) approval.

Under the CBPR system, companies in the APEC region can be certified to demonstrate their trustworthiness and accountability for personal data, facilitating the flow of data as it is transferred across the APEC region.

Not only does the referential summarise the key elements required for a BCR application and a CBPR application, but it also compares the common elements of each and where they diverge, bringing some much-needed help to international businesses trying to make sense of a complex area.

It is worth noting that the initiative is not a 'silver bullet', as businesses operating across the EU and globally still need to juggle myriad rules as to how they can use data, but it is a reminder of the need to keep on top of this fast-changing area; some developments may even be helpful. This is one new step in the right direction, being the first time that differing regulators have tried to put aside their differences in such a joined-up way.

Ensuring Compliance

The multiple recent developments, with even more to follow, should rightly fast-track data protection to the top of any business' operations, compliance and risk management agendas. It has never been more important for any business that deals with data in Europe or further afield to revisit what it is doing with its marketing, websites, customer and employee data and so on, and to check whether it is as compliant as it thinks it is.