legalweek.com
aop Digital Publisher of the Year 2010

Catching up with change - companies and evolving data protection rules

Author: Rafi Azim-Khan

11 Jan 2013 | 00:00 |

New laws, new fines and increased enforcement activity mean staying on top of data protection issues is more important for companies than ever. Rafi Azim-Khan explains

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

In the UK, for example, 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 typically a lot lower on the boardroom agenda.

All too often compliance was delegated down to a junior level and, in some cases, overlooked. But a perfect storm of different elements that have come together in recent months, including new laws, new fines, new enforcers and major new EU-wide proposals, means such an attitude is now seriously outdated and presents a risk to companies, both at national and international levels.

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

First, fines for serious breaches have been increased significantly, with each offence now potentially punishable by a fine of up to £500,000 in the UK. These new fine levels are not theoretical.

Recently, the ICO levied one fine of £440,000, one for £250,000 in September 2012 and another company was fined £325,000 in June 2012. For those who remember fine levels around the £5,000 mark, this represents a sea change.

Fine levels 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 (£811m) for data protection breaches.
Secondly, we have seen the implementation of a new E-Privacy Directive in Europe.

Such new laws increase the chance that otherwise compliant companies can be caught out as the goalposts move. In addition, an even more significant new European law is on the horizon.

One should also not underestimate the impact of a change of enforcer and enforcement priorities. We now have a new information commissioner in the UK – Christopher Graham – who is looking to

revitalise the ICO and make use of its newly increased powers. Companies should therefore be dusting off their manuals and policies as well as seeking specialist legal advice.

Worse to come?

The above elements are just the start. In January 2012, Viviane Reding, vice president of the European Commission, laid out detailed proposals for a further, major shake-up of EU DP laws.

One of the most significant announcements, and one that may keep some CEOs awake at night, is the proposal to introduce even larger fines: up to 2% of global turnover for breach of data protection law.

Companies (whether or not they are European headquartered and even if they have historically well-developed policies and procedures in place) should prioritise identifying what may need attention.

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

- personal data is processed in Europe (ie, collected and stored);
- personal data is transferred outside of Europe;
- cookies are used on websites that target European users; and
- marketing communications are sent to Europe.

Websites and social media

Aside from the increased risks of action from the ICO, one of the main reasons there is increased collection and use of data – especially via websites and social media – is the desire to process it for advertising purposes. This has driven another recent enforcement change to note.

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.

This has resulted in the Advertising Standards Authority (ASA) policing websites and social media activity. The new information commissioner was previously at the ASA and something flagged by the watchdog can equally be brought to the attention of the ICO.

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

A further well-documented shift in the law has occurred under the E-Privacy Directive, in that laws relating to the use of cookies, customer profiling and tracking data have also changed.

Users must provide consent more clearly before their data can be processed, changing the way websites operate, and there have been important EU Working Party clarifications on requirements to secure explicit, rather than implicit, consent. There has been much confusion and debate over what is or is not sufficient.

Privacy by design

The new regulation also includes the introduction of a so-called 'right to be forgotten' and the concept of 'privacy by design'.

This has been a key mantra coming out of the European Commission. Essentially, companies must now demonstrate that they are taking data protection more seriously.

When investigating a violation, enforcers are unlikely to show much sympathy for companies that have taken a lackadaisical approach to compliance. Meanwhile, updating out-of-date DP policies and retraining employees should help reduce the risks of fines.

An area under particular 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).

Multinationals sending data outside the European Economic Area have a range of options to ensure their transfers are compliant, but the solutions and the pros/cons of each are changing.

For example, when sending data to the US, 'safe harbour' has been favoured by some, despite a number of drawbacks and increased enforcement exposure. However, the use of Binding Corporate Rules (BCRs) are becoming increasingly popular among multinationals.

While the 'old' BCR regime was not that popular given a perception of slow speed and heavy workload, that view is now outdated given the introduction of the mutual recognition process. This has significantly streamlined the process and makes it an altogether more attractive option.

So, for a host of reasons, it has never been more important for any business that deals with data in Europe to urgently revisit what they are doing – what procedures, policies, standards and documents they are using, and whether they are as compliant as they think they are.

The storm of new laws, new fines and new enforcement, with even more to follow, should rightly fast-track this to the top of the boardroom agenda.

Rafi Azim-Khan (above) is a partner in Pillsbury's London office and head of the intellectual property, information technology and data privacy practices in Europe.