A "PERFECT STORM" OF DATA LAW CHANGES

- ARE YOU READY FOR A 2% OF GLOBAL TURNOVER FINE?

Recent months and the EU January announcement have seen very major data protection law changes that affect not just UK or EU companies but any companies (particularly US) which are deemed to be caught by "processing" EU data.

New fines increasing penalties from £5,000 to £500,000 per offence, implementation of the E-Privacy Directive (and new restrictions on cookie use, tracking and customer profiling), a newly appointed enforcer in the UK, new website policing for the first time and so on are already here and have helped focus attention on what has been for many a hitherto "bothersome" or "dull" compliance topic.

Increased prosecutions/fines

The push for much more aggressive fine levels and enforcement is actually the end result of too many companies taking a half hearted approach to DP (data protection) compliance, a view expressed by the enforcers along with increasing impatience and greater appetite for enforcement action.

Facebook has recently been prosecuted with the German enforcer breaking off dialogue saying that further discussions with the social media giant were "pointless".

This year will also usher in further seismic changes with proposals to beef up and alter the current main Directive. There will be numerous changes.

A key part of the new EU announcement is even larger fines - 2% of Global Turnover for DP breaches.

All of these elements are combining into quite a "perfect storm" of significantly increased risk, higher fines, more aggressive enforcers and less time to get one's house in order.

Does this affect you?

Do you process personal data in Europe? Do you really have the "consent" of the individuals whose data you process? Do you transfer personal data from Europe to the US? Do you use cookies on a website which is aimed at European customers? How about sending marketing emails to Europe – do you do this?

If any of these questions resonate with you, you should note the urgency of acting early in 2012 given this "perfect storm" of developments.

What changes might catch you out?

Firstly, it is much easier for the enforcers to fine you as some of the new powers allow "on the spot" fines without going to court. The UK Information Commissioner's Office ("ICO") has already started to use these new powers.

In terms of further developments, from 1 March 2011, social media activity as well as what you say/don't say on your corporate website became much more complex, with the regulatory Codes that did not previously apply now biting. Companies need to review their websites and use/exposure on Facebook, Twitter etc as well as how they use any data collected via the same.

Laws relating to the use of cookies and customer profile/tracking data under the EU E-Privacy Directive have also recently changed – since 6 May 2011 users must now opt in with regards to their use before they can be used/set, significantly changing the way websites operate and giving all those who conduct e-business in Europe some homework to do.

Additionally, on the issue of what constitutes "consent" there has been important EU Working Party clarification which affects the way many have been operating to date, particularly requiring explicit consent (rather than implied).

So what should you do?

"Privacy by Design" has been the mantra coming out of the EU for a while now. In order to keep enforcers at bay a company should conduct a fresh audit that highlights awareness of the recent changes, how they affect the company and related 2012 privacy by design plans/actions.

The immediate audit action item for companies (whether EU based or US but doing business in Europe) is to urgently review their current data use as well as current policies and procedures and then take corrective action.

In many cases, next steps will mean appointing/revising data privacy officers/teams and auditing how and where data is used, what consents they have/don't have and importantly what data is being transferred around the world and to where.

This last point is crucial as data transfers is a major area of change. Almost all international companies will have data transferring in a way that needs compliance with EU rules and many have what the EU increasingly regards as outdated approaches involving hundreds of (or more) Model Contracts (MCCs).

Rafi Azim-Khan
Forum Head
BritishAmerican Business Law Forum

Partner, Head IP/IT & Privacy, Europe
Pillsbury Winthrop Shaw Pittman LLP
Tel: +44 (0)20 7847 9519
Email: rafi.azimkhan@pillsburylaw.com
Website: www.pillsburylaw.com

pillsbury

The perception of the preferred alternative for group companies, Binding Corporate Rules, is also often outdated and many are unaware of the recent changes making BCRs much less costly and faster. The EU is also now very much seeing BCRs as the preferred approach for the future and there is much discussion around further BCR enhancements and "families of BCRs" proposals.

A key take-away point is that review of companies' international data transfers activities is a must.

Key 2012 Board agenda item

In short, businesses, especially US companies, that deal with data in the EU, need to urgently revisit what they are doing, what procedures, policies, standards, documents they are using and whether they are in fact as compliant as they think they are after all, given the new landscape and recent changes. The storm of new laws, new fines and enforcement, with more coming shortly, should quite rightly fast track this to the top of Board agendas. ■