

December 15, 2010

Opinion: EU needs to seize the day with fit-for-purpose privacy laws

Last year the former UK Information Commissioner Richard Thomas controversially characterised the EU's Data Protection Directive as "no longer fit for purpose", triggering a review by the European Commission.

by Bridget Treacy, head of UK privacy and information management, Hunton & Williams

The first staging post towards legislative reform was the Commission's long-awaited communication proposing "acomprehensive approach on personal data protection", published on 4 November. This is far from radical and, on some issues, is distinctly disappointing.

It contains little in the way of surprises, largely due to the Commission's efforts to ensure that its deliberations have been transparent and inclusive. There have been many opportunities for stakeholders to comment and the Commission has been willing to consult widely.

Thus, a focus on the need to increase harmonisation across the data protection laws of EU member states; clarify how the data protection principles should apply to new technologies (notably cloud computing and social networks) and promote the principles of privacy by design; simplify cross-border data transfers; enhance the rights of individuals; and increase effective enforcement by national data protection authorities, while hardly surprising, is welcome.

What is disappointing is that the review is surely an opportunity to explore more radical options for modernisation. While the commission considers the core principles of the directive to be valid, it acknowledges that the EU legal framework for data protection no longer meets the challenges of technological development and globalisation.

These challenges are significant. At the 32nd International Conference of Data Protection and Privacy Commissioners, held in Jerusalem in October, the Israeli commissioner asked delegates to consider whether secrets still remain secret in a digitised world, or whether the digital explosion has meant that our privacy rights have already been compromised.

The commissioner calculated that in 2010 more than 1.2 zettabytes of information will be created on blogs and social networks — the equivalent of broadcasting every day for 125-million years. Notwithstanding this, newer approaches to data protection regulation, including the potential role of an accountability principle, receive only tentative support from the Commission.

More radical thinking will be required, including a move away from the current approach of mandating prior approvals for data processing.

An accountability principle is one such approach. Crucially, it is not a substitute for legal compliance, but would require an organisation to implement measures to show it complies with

existing regulations, industry codes and its own promises. This is not far removed from the approach many data protection authorities encourage organisations to adopt.

Widespread adoption would probably require incentives in conjunction with sanctions. A reduction in prior approval mechanisms and bureaucratic form-filling might provide a sufficient incentive, while fines or mandatory audit and remediation might well act as sufficient deterrents.

Of course, these proposals are not new. They reflect a contemporary approach to regulation and compliance. Organisations should already recognise that personal data is a core corporate asset that must be safeguarded. Consumers regard data breaches as serious breaches of trust.

The Commission's paper is by no means the last word on possible reform and comments are invited by 15 January 2011. Legislative proposals are expected to follow towards the end of 2011. Now is the time to have your say.