Commission reports uneven playing field for data protection

Kate Brimsted looks at the findings from the European Commission's investigation into the implementation of the EU Data Protection Directive.

On May 16th, the European Commission published its first report on the implementation of the Data Protection Directive (95/46/EC). The report is based on a review of EU member states' data protection laws, a wide consultation exercise which included an international conference, and an online survey that generated over 10,000 responses (*PL&B International*, Nov 2002, p.6).

The essential questions to be addressed by the report were whether the ways in which the member states have transposed the directive into national law achieve the ambitions of the directive. If not, what should be done to correct this? For example, should the directive itself be amended?

Several of the member states have been late in implementing the directive and France was singled out for criticism by Internal Market Commissioner, Frits Bolkestein, as it is still relying on data protection legislation dating back to 1978.

THE OVERALL PICTURE

The Commission expressed general satisfaction with the implementation of the directive and there are no current plans to amend it. However, the Commission recognised that, so far as ensuring a level playing field for operators in different member states and simplifying the regulatory environment, the differences between member states' laws and the directive are still too great. Amendments to national legislation are likely to be required in due course (this will be the subject of future reviews).

The Commission has proposed a work programme to address divergences in implementation and raise awareness.

SPECIFIC AREAS OF DIFFICULTY IDENTIFIED IN THE REPORT

The Commission's report highlighted the following key findings:

Sensitive and non-sensitive personal data - greater clarity on the "legitimate interests" condition was sought - this condition allows processing of non-sensitive personal data by data controllers without the subject's consent, provided that the legitimate interests, rights and freedoms of the individual are not overridden.

The Commission's view is that the absence of adequate safeguards means appropriate levels of protection for individuals are not currently being achieved.

> The Commission felt that [notification] problems were largely due to member states' failures to carry through the exemptions available in the directive.

Applicable data protection law – this topic came in for heavy criticism by respondents as, currently, organisations with a presence in (or which merely "use equipment" to process personal data in) more than one member state may have to comply with multiple national data protection laws. Submissions received argued for a "country of origin rule", allowing multinationals to operate via one set of rules throughout the EU. The Commission agreed that this area, and the term "use of equipment" in particular, needed clarification.

Legitimate processing conditions – these have been implemented unsatisfactorily in a number of jurisdictions, raising issues concerning appropriate safeguards and grounds for legitimate processing. In particular, the distinction between "unambiguous consent" (one of the conditions for lawful processing of non-sensitive personal data) and "explicit consent" (which is the level of consent required to process sensitive personal data) needs to be clarified to ensure uniformity across member states.

Provision of information to data subjects – in some jurisdictions, the law (wrongly) requires that certain "fair processing" information (for example, ensuring the data subject knows who the data controller is and the purposes for which his personal data are being processed) always has to be provided to the data subject, regardless of whether the individual already has that information or not. This causes significant difficulties for multinational companies doing business at pan-European level, especially via the Internet.

Notification requirements – many respondents argued that the notification process should be simplified on the grounds that it imposes a huge administrative burden on controllers without a commensurate improvement in protection for data subjects. The Commission felt that problems were largely due to member states' failures to carry through the exemptions available in the directive. For example, one such exemption currently under-employed by member states is the ability for controllers to appoint company privacy officers as an alternative to notification.

Exporting data outside the EEA – member states have diverged greatly on this business-critical issue. The directive mandates that (unless exempt) personal data may be transferred only to countries which ensure an adequate level of data protection. At present, some member states require almost no reference to be made to the national supervisory authority, whereas others require everything to be referred for authorisation, even where exemptions apply. The effect of this is likely to be that data exports will "switch to the 'least burdensome' point of export."

Subject access requests - despite calls for more flexible interpretation by those consulted, the Commission was not convinced (surprisingly, in the author's view) that this aspect of the directive was posing serious practical problems for controllers. The Commission relied on the 62 per cent of data controllers whose responses to its online questionnaire indicated that responding to subject access requests did not constitute an important effort for their organisation. However, as most of the respondents apparently either had no figures available or had received fewer than ten requests, it is possible that their responses reflect a lack of experience.

Future Plans

In response to concerns identified in the report, including on the levels of compliance, enforcement and awareness, the Commission intends to put in place a number of initiatives. A work programme for 2003-4 has been proposed which will include discussions between the Commission, member states and national data protection authorities. The Commission has also called for the Article 29 Data Protection Working Party to draw up proposals for a substantial simplification of notification requirements, more harmonised information requirements and for simplifying the international data transfer regime. Promoting PETs (Privacy Enhancing Technologies), self-regulation and raising awareness of data privacy rights were also highlighted as targets for improving data protection.

What changes can businesses expect to see?

Over the short-to-medium-term, the call for increased resources for national data protection authorities and initiatives to heighten the public's awareness of data protection rights can be expected to raise the compliance stakes for data controllers throughout the EU.

The sooner organisations put in place compliance programmes, the better the position they will find themselves in once the anticipated tougher enforcement regimes become a reality.

The outlook is not just weighted in favour of individuals however. At a detailed level there is recognition that the lack of consistency in data export restrictions, applicable law and notification obligations needs to be addressed.

So far as the notification regime is concerned, this can undoubtedly be simplified and one would expect the "data privacy officer" role to become more widely recognised in member states. This can be predicted to have a significantly beneficial impact on the corporate data privacy environment.

Regarding data exports, the Commission expects to see progress in four key areas: (1) more "approved country" findings; (2) a wider choice of recognised standard clauses for data export contracts; (3) the role of binding intra-corporate rules eg. group-wide data protection policies; and (4) more uniform interpretation of the exemptions. This will be heartily welcomed by businesses and can only promote smooth international data flows, with all the enhancements in information use and efficiencies these entail.

AUTHOR: Kate Brimsted is a senior assistant solicitor in the IP & Technology Department at Herbert Smith and a member of Herbert Smith's Data Privacy Working Group. She can be contacted via e-mail: kate.brimsted@herbertsmith.com

FURTHER INFORMATION: A copy of the Commission's report can be found at: http://europa.eu.int/comm/internal_market/privacy/lawreport_en.htm

EU survey reveals consumer discontent

Between June and September last year, the European Commission launched an online consumer consultation into the impact of the EU Data Protection Directive. The survey received 9,516 responses with the majority coming from Germany, France and the UK.

Analysis of the survey - recently published on the Commission's website - suggests consumers consider that governments are placing business concerns ahead of citizens' privacy rights. They believe that businesses are getting away with data protection breaches 'scot-free' and are especially concerned that health insurance companies are improperly collecting data from their doctors.

The report highlighted a general call for tougher regulatory sanctions with some respondents expressing the view that data protection authorities do not have enough powers.

Workers are happy to have e-mails read by their employers but only if they are business-related. One solution proposed by respondents was to provide workers with both a private and business e-mail address.

Some of the key figures from the survey include:

- 45 per cent consider their country to be providing a good-high level of protection
- 5 per cent think that there is not a good enough level of awareness among consumers
- 66 per cent are concerned that their personal data will be misused when using online services
- 56 per cent would like to see a positive opt-in rule for e-marketing
- 84 per cent are aware of 'invisible' data collection through the use of cookies and spyware technologies.