Editorial

Bridget Treacy considers the 2009 privacy agenda thusfar, for Volume 9, Issue 4, of Privacy & Data Protection

We have only reached March and already the 2009 privacy agenda is packed full of initiatives and issues to ponder. These initiatives centre on the key privacy tension of maximising the use of personal data, whilst reassuring individuals that their information is safeguarded and processed in accordance with their rights.

During February, the Information Commissioner's Office ('ICO') launched its much debated Personal Information Promise. The Promise consists of a set of ten statements about data protection practices which the signatory organisation promises to uphold. The Promise must be signed by a senior executive, and the names of organisations that have signed are listed on the ICO's website. Some organisations have expressed concern that signing the Promise will expose them to greater data protection risk. In particular, the Promise commits the organisation to "go further than just the letter of the law when it comes to handling personal information," and to "treat it as a disciplinary matter" if staff fail to safeguard personal information. The ICO's website clarifies that it does not intend to bring enforcement proceedings on the basis of the Promise, but companies with a US parent are only too familiar with Section 5 of the Federal Trade Commission Act which enables the Federal Trade Commission to bring enforcement proceedings on the basis of conduct in trade (including a privacy statement or promise) which is misleading or deceptive. For other organisations which are data processors rather than data controllers, the Promise may extend the obligations beyond those of a processor under the Data Protection Act ('DPA'). Further, companies have commented that before signing the Promise, a senior executive will be required to provide reassurance that the Promise can be met. This is presumably the purpose of the initiative. It raises the profile of data protection within an organisation, at a senior level, and within the public domain. The fact that the Promise has generated so much discussion in the market suggests its objective has already been met.

February has also seen much debate within the Public Bill Committee on the Coroners and Justice Bill, which proposes amendments to the DPA. The most controversial provisions are those relating to data sharing, which may result in data collected by the public sector being shared with the private sector, and processed for different purposes. Further, the Bill introduces additional powers for the Information Commissioner, including the power to serve Assessment Notices (via section 151, which states "an Assessment Notice will allow us to inspect an organisation to determine whether it is complying with the data protection principles"). In its current form the section allows Assessment Notices to be served on "a government department or designated public authority [but not] a private or third sector organisation." The Commissioner has already signalled that this power should be extended to the private sector, and that sanctions should be established for failure to comply with an Assessment Notice. The ICO's comments underline a greater concern to ensure that data processing is transparent and that individual's rights are safeguarded.

At the European level, the Article 29 Working Party has published two papers on key issues: one addresses the difficulty of responding to pre-trial discovery in cross border litigation (discussed in greater length in the next Editorial); the other comments further on current proposals to amend the e-Privacy Directive, including the scope of its proposed data breach notification requirement (see pages 8 to 11 of this edition). On the data breach front, the Working Party's Opinion suggests that the breach notification obligation included in the proposed amendments to the e-Privacy Directive should encompass information society services, and not just internet service providers. The effect of such an amendment would be to impose a data breach notification obligation on the providers of all online services such as banks, retailers, healthcare providers, and many others. Data breach, and the possibility of a data breach notification law, has been discussed in great detail following the series of significant data breach incidents in Europe in the last twelve months. A more general data breach law now appears inevitable.

Organisations may be ever more creative in devising ways of maximising their use of personal data, but the data protection regulators remain resolutely focused on safeguarding the rights of individuals. The privacy agenda will continue to challenge us all. In the next Editorial we will focus on privacy notices, the Working Party Opinion (referred to above) on cross border litigation, and the recent developments made by the Asia-Pacific Economic Cooperation Data Privacy Subgroup.

Bridget Treacy
Editor and
Partner at Hunton & Williams
btreacy@huntonandwilliams.com