Introduction
The Information Commissioner's Office (ICO), the UK watchdog for data privacy issues, this week published a draft code of practice on privacy impact assessments (PIAs). The draft code explains the functions of PIAs and provides useful guidance to organisations on how they should be conducted. Publication of the draft code follows enforcement action taken by the ICO last month against the police where a breach of the Data Protection Act 1998 (DPA) could have been avoided had a PIA been conducted.

Privacy Impact Assessments
A PIA is a process for evaluating a project or scheme to identify its potential effects upon individual privacy and data protection compliance and to examine how any detrimental effects might be overcome.

According to the draft code, organisations should carry out PIAs at a time when new projects are planned, or when revisions are intended to existing practices. Businesses conducting PIAs should ensure that their project plans are sufficiently flexible to allow for amendment in the event that the PIA identifies privacy issues that need to be addressed.

Crucially, there is no statutory requirement for an organisation to complete a PIA – although central government departments have been instructed to complete PIAs by the Cabinet Office – but the ICO advocates their voluntary use and the draft code follows previous ICO guidance that it has issued on how and when PIAs should be carried out.

Recent Enforcement Action
From the ICO's perspective, PIAs represent an opportunity for firms to identify the impact upon privacy that a project will have and, ultimately, prevent breaches of the DPA. Recently, the ICO took enforcement action against Hertfordshire Constabulary in circumstances where breach of the DPA by the police could have been avoided had a DPA been conducted.

The Constabulary had installed automatic number plate recognition (ANPR) cameras to monitor traffic going in and out of the town of Royston. In a landmark decision, the ICO declared the practice to be unlawful and ordered the Constabulary to cease all processing of information recorded by the cameras immediately and not to resume until an assessment of the risk to individuals’ privacy has been conducted which demonstrates that the practice is in compliance with the requirements of the DPA.

The system was deemed to be unlawful by the ICO because license plates and other vehicle registration marks constitute personal data under the DPA and, as such, the Constabulary was under a duty not to process personal data that was excessive in relation to the purpose or purposes for which it was collected originally. In addition, the practice was found to be a violation of the vehicle license plate holders’ right to privacy under Article 8 of the European Convention of Human Rights.

The enforcement notice served upon the Constabulary states that the PIA should: define the pressing social need for the ANPR system; assess the likely effectiveness of the proposed measures in addressing that need; identify the likely impact of the activity on the private lives of individuals; and determine that the proposed measures are a proportionate interference.

Should I conduct a PIA?
The case provides a clear example of the value to organisations in planning effectively the ways in which they intend to use the personal data that they collect and, in particular, by conducting PIAs. The ICO made clear that the breach of the DPA could have been avoided in this case had a PIA been carried out prior to the surveillance system being installed. The Constabulary will now have to invest a considerable amount of time and expense to become compliant with the DPA.

Whilst businesses may be reluctant to invest additional time and resources in data privacy processes, PIAs give organisations the opportunity to identify and manage risks from an early stage,
avoid inadequate solutions and unnecessary costs, avoid loss of trust and reputation (if incidents occur), and gain an understanding of the perspectives of stakeholders.

**Legislative Reform**

Organisations should also be aware that, under current proposals being considered in the European Parliament, there is a real prospect that PIAs will soon become mandatory. The proposed draft of the EU General Data Protection Regulation (the ‘proposed Regulation’) provides for a PIA to be carried out "(W) here processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes…”.

The proposed Regulation identifies operations which carry particular risks that would necessitate a PIA being carried out (these include video surveillance on a large scale) and sets out minimum requirements as to what a PIA must comprise. The ICO has endorsed these provisions and has gone further by advocating for an additional provision requiring organisations to publish summaries of the PIAs they carry out. It should be noted, however, that the final text of the proposed Regulation is still being considered and remains subject to further amendment prior to its anticipated entry into force in 2015.

**Conclusions**

The release of the new ICO draft code and the Hertfordshire Constabulary case demonstrate the importance that the ICO attributes to PIAs and their potential value in providing an early warning to organisations that their activities will not be DPA compliant.

In light of this, and the proposed Regulation potentially making PIAs mandatory, we would recommend that when organisations are planning new projects involving data processing operations they should factor into their project planning consideration of whether a PIA will be necessary.

The draft code is open to consultation until 5 November 2013.

If you are interested in exploring how the issues raised above will affect your business, please contact your usual Pinsent Masons adviser, or:

**Marc Dautlich**
Partner
London
T: +44 (0)20 7490 6533
M: +44 (0)7984 405672
E: marc.dautlich@pinsentmasons.com