COVINGTON

COVINGTON & BURLING LLP

ADVISORY | Global Privacy & Data Security

December 21, 2010

UNITED KINGDOM

UK Information Commissioner Wields First Fines for Violations of Data Protection Act

On 24 November 2010, the UK Information Commissioner's Office ("ICO") issued its first fines for breach of the Data Protection Act 1998 since its extended enforcement powers came into effect in April. The first penalty of £100,000 was imposed on Hertfordshire County Council after it negligently released sensitive personal information, including information relating to a child sex abuse case, to unintended recipients on two separate occasions. The second fine, of £60,000, was imposed on an employment services company following the theft of an unencrypted laptop that contained sensitive information on thousands of individuals who had used community legal services, including information about alleged criminal conduct. Both organizations self-reported the incidents to the ICO.

The ICO has ruled that the monetary penalties were entirely appropriate, on the basis that access to the information, which was highly sensitive in nature, could have caused substantial distress to individuals. It was also clear that both organizations failed to implement adequate security to prevent the incidents from occurring. While far from the maximum possible penalty of £500,000, the fines are an important development and signal a change in approach by the ICO, which has traditionally demonstrated reluctance in using a heavy handed approach to enforcing compliance. That said, the level of fines imposed in these particular cases suggests that only exceptionally serious violations are likely to merit the top-level fine.

The ICO Press Release can be viewed at:
http://www.ico.gov.uk/~/media/documents/pressreleases/2010/first_monetary_penalties_press_release_24112010.ashx

OTHER EUROPEAN DEVELOPMENTS

Council of Europe issues Recommendation on Profiling

On 23 November 2010, the Council of Europe adopted a recommendation (the "Recommendation") on the "protection of individuals with regard to automatic processing of personal data in the context of profiling." The Recommendation is designed to apply the principles and protections established by Convention 108 to consumer profiling activities. The term "profiling" is defined as "an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning him or her or for analyzing or predicting his or her personal preferences, behaviours and attitudes." The Recommendation advocates, inter alia, the following practices: (i) the use of privacy-enhancing technologies ("PETs") and the control of technologies designed to circumvent PETs; (ii) the establishment of a clear legal basis to engage in profiling activities (in this respect, when relying on consent, the burden rests with the organization conducting the profiling to show that the individual furnished informed consent); (iii) allowing consumers access to goods and services without the need to furnish personal information to service providers and without the use of

default profiling; (iv) periodic checks to ensure data quality and to ensure that any inaccuracies in any personal information are corrected; and (v) restrictions on the use of sensitive personal information for profiling.

The Recommendation is a major development in seeking to create a set of general rules for profiling activities and represents the outcome of a long series of ministerial discussions and stakeholder input on this issue. Although the Recommendation does not have binding effect, it encourages members to implement its principles into law and to promote industry self-regulation in this area, for example, by developing codes of conduct.

The Recommendation can be viewed at:
https://wcd.coe.int/wcd/ViewBlob.jsp?id=1710949&SourceFile=1&&BlobId=1712512&DocId=1663576&Index=no

INTERNATIONAL

Proposals to Toughen Hong Kong's Privacy Regime

Hong Kong-based businesses are facing proposals that would substantially strengthen the Hong Kong privacy landscape. Government officials have announced proposals that, if implemented, will amend Hong Kong's Personal Data (Privacy) Ordinance (the "Ordinance") to include, inter alia, new restrictions on direct marketing, tougher data security standards and more meaningful enforcement powers for the Hong Kong data protection regulator. Stakeholders have urged government officials to consider the potential negative impact of the changes on Hong Kong's business community. The public consultation report, which sets out 37 potential revisions to the Ordinance, can be viewed at:
http://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

New Zealand Favoured for Adequacy Assessment

The Article 29 Working Party, the influential data protection advisory body, has revealed that it will consider whether New Zealand's legal regime provides adequate protection for the personal information of EU citizens at its December 7-8 meeting this year in Brussels. While a positive assessment by the Article 29 Working Party is useful towards achieving official "adequacy" status, this process requires that the European Commission issue a formal adequacy decision, which may or may not take account of the Working Party's views. Achieving a positive adequacy determination will mean that it will be possible for organizations to send personal information freely to any New Zealand-based entity or person without the need to complete additional formalities (such as standard model contracts or regulatory authorizations, for example). The European Commission has thus far recognized only a small number of countries as having adequate data protection regimes, including Israel, which received a positive adequacy ruling this October.

At the December meeting, the Working Party will also spend time considering the recent Commission Communication on a "comprehensive approach on personal data protection in the European Union," which lists more than 35 proposals for change to the existing data protection regime. In particular, the Working Party will give consideration to developing opinions on the concept of sensitive data and the regime for notifying the processing of personal data, to address obvious maladies in the system and further fuel the debate over the future course of privacy law.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our global privacy & data security practice group:

Daniel Cooper	+44.(0)20.7067.2020	dcooper@cov.com
Jetty Tielemans	+32.2.549.5252	htielemans@cov.com
David Fink	+32.2.549.5266	dfink@cov.com