Privacy and Security Alert: Privacy Law Developments in the United Kingdom: New Powers To Levy Fines for Personal Data Breaches

3/11/2010

By Susan L. Foster

The United Kingdom's Information Commissioner's Office (ICO) will soon have the ability to levy fines of up to £500,000 for significant breaches of the Data Protection Act 1998 (DPA). The new fines may be imposed when the breach of the DPA is serious in nature, and the breach was deliberate or reckless and likely to cause substantial damage or distress to an individual. The fines are scheduled to come into effect on April 6, 2010.

Who Is at Risk?

The DPA applies to individuals and companies based in the United Kingdom that handle personal data of residents of the UK. The DPA also can apply to companies that are based outside of the UK, depending on the circumstances (such as U.S. Safe Harbor membership or a contractual agreement). It is worth noting that the fines apply to data controllers (those who determine how personal data is collected and used) and not to data processors (individuals or organizations that process data at the direction of a data controller). However, a data controller can be fined on the basis of the acts of its data processors. This is particularly a risk if the data controller does not have a contractual agreement or the equivalent in place with the data processor, or fails to check that the data processor is complying with its contractual obligations regarding personal data.

How Can the Risk of a Fine Be Minimized?

The purpose of the ICO's new ability to levy fines is to deter and punish serious non-compliance with the DPA. The ICO's guidance focuses on "deliberate" and "reckless" breaches.

Deliberate breaches should be fairly easy to avoid. However, even generally responsible companies may be concerned by the standard for "reckless" non-compliance. The ICO will ask whether the data controller *knew or should have known* that there was a risk of a breach of a kind likely to cause substantial damage or distress. If so, the ICO will ask whether reasonable steps were taken to prevent the breach.

In light of the ICO's guidance, companies handling UK personal data should strongly consider carrying out risk assessments on a regular basis. Companies should put measures in place to address any risks that they identify relating to the loss or misuse of personal data.

Guidance on Laptops and Portable Devices

One particular example in the guidance of "reasonable steps" may make IT and privacy officers flinch: Does the company have appropriate policies and procedures in place—such as the encryption of all laptops and removable media (such as flash drives) — to avoid loss of personal data if an employee's laptop or removable media is stolen? IT officers might also need to consider how to secure personal data on Blackberry™ and other personal devices. Failing to do so might be considered "reckless" depending on the likely consequences of the loss of personal data contained in the unsecured devices.

What Can You Do if You Receive Notice of a Fine?

Before imposing a fine, the ICO will give a company written notice specifying the details of the alleged breach and the amount of the fine. The company then has 28 days to respond to the ICO, and can submit documents supporting a request to reduce or retract the fine. The ICO may then retract the fine or impose part or the full amount of the initially proposed fine. Furthermore, the ICO will publish the fine and the company's name on the ICO website. The company can appeal the fine, but the current guidance suggests that the company cannot prevent publication on the ICO website once the ICO makes its final decision to impose the fine.

UK Guidance

The ICO has published detailed guidance concerning when fines will be issued, the process for trying to get fines withdrawn or reduced, how to appeal, and payment. See the Information Commissioner's guidance about the issue of monetary penalties, here.

For assistance in this area please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

R. Robert Popeo
(617) 348-1716
RRPopeo@mintz.com

Cynthia J. Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Dianne J. Bourque
(617) 348-1614
DBourque@mintz.com

Susan L. Foster, Ph.D.
+44 (0) 20 7776 7330
SFoster@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Haydon A. Keitner
(617) 348-4456
HAKeitner@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com